الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA
BADJI MOKHTAR - ANNABA UNIVERSITY



جامعة باجي مختار – عنابـــة

كلية الحقوق و العلوم السياسية

القسم: العلوم السياسية

الميدان: الحقوق و العلوم السياسية

الشعبة: العلوم السياسية

التخصص: إدارة عـــامة

مذكرة

مقدمة استكمالا لمتطلبات نيل شهادة الماستر

دور الأجهزة الأمنية الجزائرية في محاربة الجريمة الإلكترونية

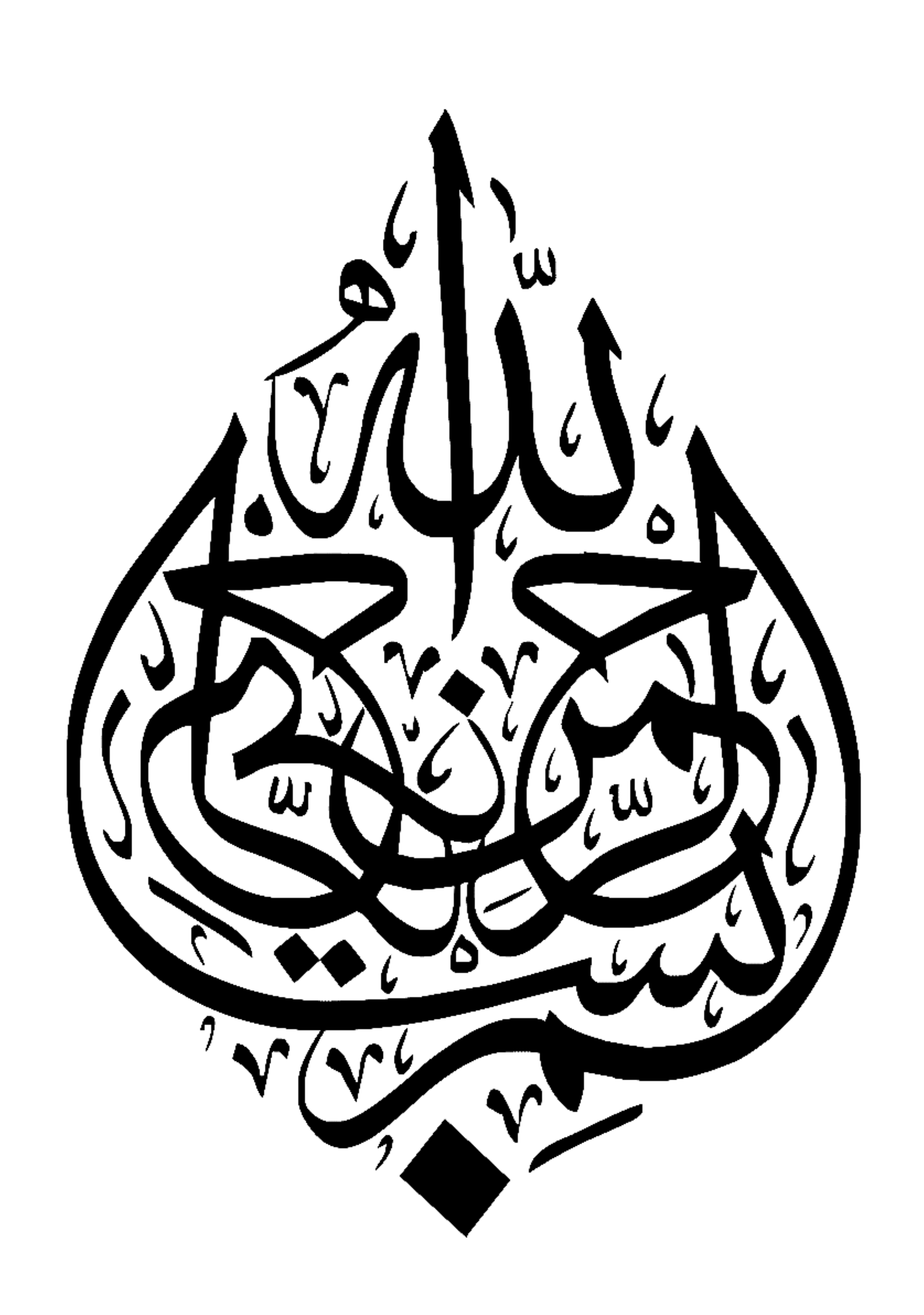
إعداد الطالب: عبد العلي شواكرية

إشراف الأستاذ: عبد الله حرابي جامعة عنابة

لجنة المناقشة:

الصفة	الجامعة الاصلية	الدرجة العلمية	اسم ولقب الاستاذ
رئيسا	جامعة عنابة	أستاذ محاضر (ب)	وحيدة بورغدة
مشرفا ومقررا	جامعة عنابة	أستاذ مساعد (أ)	عبد الله حرابي
ممتحنا	جامعة عنابة	أستاذ مساعد (أ)	هشام زغاشو

السنة الجامعية: 2021/2020


بسم الله الرحمن الرحيم



إهداء

إلى من أفضلها على نفسي ولم لا، فلقد ضحّت من أجلي، ولم تدخر جهدا في سبيل إسعادي على الدوام **(أمي الحبيبة)**.

نسير في دروب الحياة، ويبقى من يسيطر على أذهاننا في كل مسلك نسلكه.

صاحب الوجه الطيب والأفعال الحسنة، فلم يبخل علي طيلة حياته

(والدي العزيز).

إلى **زوجتي الحبيبة** التي وقفت معي في كل الأوقات الصعبة وكانت سندي ومصدر قوتي.

إلى قرة عيني بناتي **"ميلينا"** و**"شهد"**.

إلى إخوتي **"هواري"**، **"نوال"**، **"فؤاد"**، **"رؤى"**، **"صفاء"** و**"حسام الدين"**.

إلى روح الفقيدين العزيزين على قلبي **"جد"** و**"جدة"** بناتي

"عبد الحكيم" و**"سهام"** رحمهم الله وأسكنهم فسيح جناته.

أهدي لكم هذا البحث وأتمنى أن يحوز على رضاكم.

عبد العالي



شكر وتقدير

قال تعالى: (وَمَن يَشْكُرْ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِ) "لقمان – 12"

أحمد الله تعالى حمدا كثيرا طيبا مباركا ملئ السماوات والأرض على ما أكرمني به من إتمام هذه الدراسة التي أرجو أن تنال رضاه.

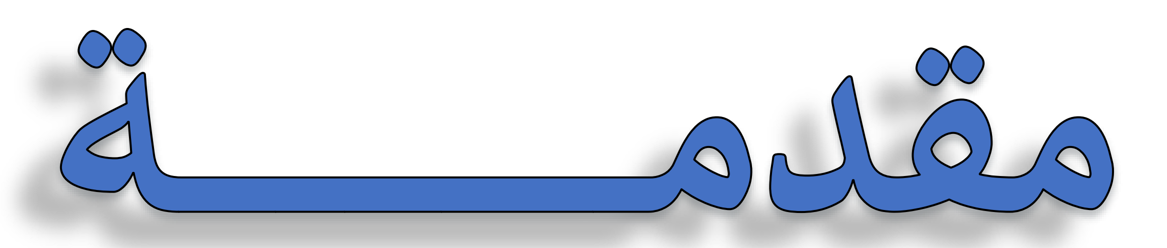
أتوجه بجزيل الشكر وعظيم الامتنان إلى كل من:

- الأستاذ الفاضل **"عبد الله حرابي"** لقبوله الإشراف على هذا البحث، وتكرمه بالنصح والإرشاد وتوجيهاته القيمة التي ساهمت في اثراء موضوع دراستنا في جوانبها المختلفة، كما أتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة الموقرة.
- إلى جميع **الأساتذة** الذين أشرفوا على تدريسي خلال مساري الجامعي وكل **موظفي وعمال** الكلية.
- إلى رئيسي في العمل، محافظ الشرطة السيد: **"أحمد شوقي سعايدية"** على وقوفه بجانبي وتقديمه يد العون والمساعدة لي في كل الظروف، والذين بدونه ما كنت أتممت هذا البحث.
- إلى **"زملائي في العمل"**، على كل ما قدموه لي من دعم وتشجيع، لكم مني كل الشكر والإمتنان.
- إلى صديقي **"دوخي محمد أمين"** على وقوفه بجانبي طيلة مساري الدراسي وإمداده لي بالنصح والإرشاد.

الفهرس

قائمة الجداول

قائمة الأشكال


مقدمة

رغم الإيجابيات التي تحملها التطورات التكنولوجية، إلا أنها حملت معها العديد من التهديدات والمخاطر التي ترجمت في الجرائم الإلكترونية التي لا تفرق بين الأشخاص والمؤسسات والدول، فلا ينكر أحد الدور الكبير لشبكة الأنترنت في حراك الشعوب العربية.

وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحى تصاعديا في الآونة الأخيرة، وهو ما ينبأ بخطورة الوضع، لا سيما في ظل ما تشهده السنوات الأخيرة من تسارع في مجال تكنولوجيات الإعلام والإتصال، كاستخدام تطبيقات الأنترنت ووسائل التواصل الإجتماعي والدفع الإلكتروني ...إلخ.

وهذا ما جعل السلطات الجزائرية تتخذ جملة من الآليات القانونية والتشريعية لمحاربة هذه الظاهرة وإنشاء هياكل تنظيمية خاصة، مع تولي الأجهزة الأمنية المتخصصة مسؤولية الوقاية ومكافحة هذه الظاهرة من خلال التعامل مع المتغيرات الحديثة والتكيف معها، لتسهيل عمليات التحقيق وكشف المجرمين وتسليمهم للعدالة.

1- دوافع اختيار الموضوع:

هناك جملة من الدوافع الذاتية والعلمية التي جعلتني أختار موضوع دراستي أذكر منها:

أ- الدوافع الذاتية:

- الدراسة لهذا الموضوع من شانها أن تعزز وتثري معارفي القانونية حول الجريمة الإلكترونية.
- اهتمامي بالدارسات الأمنية، فانطلاقا من طبيعة عملي بسلك الأمن الوطني جعلني أهتم بموضوع الجريمة الإلكترونية.
- الرغبة في إكتشاف ومعرفة الصعوبات التي تواجهها الأجهزة الأمنية المتخصصة، أثناء عملها في محاربة الجرائم الإلكترونية.

ب- دوافع الموضوعية:

- كثرة الجرائم الإلكترونية التي يتعرض لها المستخدمون عبر الأنترنت ووسائط التواصل الإجتماعي المختلفة، مثل الفايس بوك.

- الإطلاع على أهم السياسات الوطنية والدولية التي تبنتها الجزائر من أجل الحد من إنتشار الجرائم الإلكترونية.
- تسليط الضوء على أهم المؤسسات الأمنية المننوط بها الإستراتيجية الوطنية لمحاربة الجريمة الإلكترونية.
- إختبار المعارف المنهجية المكتسبة طوال المسار الدراسي.

2- أهمية البحث:

يعد موضوع البحث من الموضوعات الحديثة والمهمة في نفس الوقت، حيث لا تزال الدراسات والبحوث فيه متواصلة من اجل الإحاطة بمختلف جوانبه، وقد وجدت لهذه الدراسة التي قمت بها أهمية علمية وأخرى عملية تتمثل فيما يلي:

أ- **الأهمية العلمية:** تندرج الدراسة ضمن حقل الدارسات الأمنية والإستراتيجية، وتتجلى أهميتها العلمية في كونها تتناول موضوعا حديثا يرتبط إرتباطا وثيقا بالواقع الذي نعيشه داخل مجتمعنا، والذي يتطلب منا فهما أوسع لطبيعة الجريمة الإلكترونية ومختلف أشكالها وكيفية إرتكابها، وما هي أهم التشريعات القانونية والمؤسسات الأمنية التي جاءت بها المنظومة الوطنية في إطار مكافحة الجرائم الإلكترونية، كما يزيد من أهمية الدراسة فهم التهديدات الخطيرة التي يتعرض لها الأمن القومي للبلاد.

ب- **الأهمية العملية:** تعد الجريمة الإلكترونية من الظواهر التي أصبحت تمثل الواقع المعاش من خلال وقوع العديد من مستخدمي الأنترنت ضحايا لها، لذلك كان لابد من معرفة الأساليب والأنواع المختلفة لهذه الجريمة من أجل تجنب الوقوع فيها، والإطلاع على القوانين التي تجرمها وتحمي حقوق الأفراد كذلك التعرف على السياسة الأمنية الوطنية المنتهجة والأجهزة المكلفة بمكافحتها وطرق وأساليب عملها للإطلاع على مدى فعاليتها في الميدان.

3- أهداف الدراسة:

يعتبر مجال البحث العلمي مجالا واسعا تختلف أهدافه وتتعدد معطياته، حيث يهدف تبني أي باحث لموضوع معين محاولة لإشباع فضوله المعرفي الذي يلازمه وإزالة الغموض عن بعض القضايا، لذلك تهدف دراسة "دور الأجهزة الأمنية في محاربة الجريمة الإلكترونية" إلى الأهداف التالية:

- التعرف بمختلف أنواع الجرائم الإلكترونية المرتكبة والتي تستهدف مستخدمي الأنترنت ووسائط التواصل الإجتماعي.
- إبراز المجهودات الدولية والوطنية المبذولة من أجل مواجهة مختلف الجرائم الإكترونية.
- اظهار إستراتيجية الأجهزة الأمنية الجزائرية في محاربة الجرائم الإكترونية.
- تقديم بعض التوصيات والمقترحات التي من شأنها تعزيز الإستراتيجية الوطنية في مكافحة الجرائم الإكترونية.

4- إشكالية البحث:

بالرغم من إنخراط الجزائر في الجهود الدولية لمكافحة الجرائم الإلكترونية ووضعها للآليات قانونية ومؤسساتية وطنية للقضاء والحد من إنتشارها الواسع، إلا أنه لا تزال المصالح الأمنية المتخصصة تسجل إرتفاعا متزايدا لعدد ضحايا الجريمة الإلكترونية.

وعليه فالإشكالية الرئيسية لهذه الدراسة هي:

ما مدى فاعلية الأجهزة الأمنية الجزائرية في مكافحة الجريمة الإلكترونية؟

ومن هذا السؤال نطرح التساؤلات الفرعية التالية:

- ماهي طبيعة الجريمة الإلكترونية وكذا سمات المجرم الإلكتروني وما مدى تأثيرها على الأمن السيبراني؟
- ما هي الأجهزة الأمنية الجزائرية المكلفة بمحاربة الجريمة الإلكترونية؟
- ماهي أهم المعوقات التي تحول دون تحقيق الإستراتيجية الوطنية لمحاربة الجريمة الإلكترونية؟

5- فرضيات البحث:

- كلما زاد التطور التكنولوجي في مجال الإتصال والمعلومات، كلما زادت الجرائم الإلكترونية.
- على الرغم من تطوير الأجهزة الأمنية وبذلها الكثير من الجهود، إلا أنها لم تستطع مواجهة الجريمة الإلكترونية والقضاء عليها.
- كلما زاد التركيز على تطوير الأجهزة الأمنية، كلما قل إنتشار الجريمة الإلكترونية بالجزائر.

6- حدود الدراسة:

إن لكل موضوع بحث حدود تحدد معالمه وتربطه بالمكان والزمان الذي جرت فيه الدراسة البحثية، حيث جاءت حدود دراستنا كما يلي:

أ- الحدود الموضوعية:

تهتم دراستنا البحثية بالسياسة الأمنية الجزائرية المنتهجة في مكافحة الجريمة الإلكترونية ومدى تفاعل الأجهزة الأمنية معها في الميدان.

ب- الحدود المكانية:

تهتم دراستنا بدور الأجهزة الأمنية الجزائرية في مكافحة الجريمة الإلكترونية، وبالتالي تمثل **"الجزائر"** حدود هذه الدراسة.

ج- الحدود الزمانية:

ويتمثل في المرحلة التي مر بها البحث، وهي الفترة الممتدة من بداية شهر فيفري 2020 الى غاية شهر جوان 2021.

7- الدراسات السابقة:

إن أية دراسة علمية أو بحث أكاديمي يتطلب الرجوع والإطلاع على الدراسات السابقة في نفس المجال وهذا لفهم الموضوع وتوجيه الباحث للمسار الصحيح، ومن الدارسات السابقة التي رجعت إليها بغرض الاستفادة:

- دراسة لـ نعيم سعيداني بعنوان " آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري":

مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، قسم الحقوق، كلية القانون والعلوم السياسية، جامعة الحاج لخضر- باتنة- سنة 2012-2013، حيث تناولت الدراسة الإشكالية التالية: هل استجاب المشرع الجزائري لهذه المبررات واستحدث في سبيل ذلك تشريعات جديدة

لمعالجة آثار وانعكاسات التقنية المعلوماتية على إجراءات البحث والتحري وإلى أي مدى وفق المشرع في إستحداث طرق إجرائية في سبيل البحث والتحري عن الجريمة والمجرم المعلوماتي؟ حيث حاول أن يحصر نطاق هذه الدراسة ضمن خطة تتكون من فصلين تطرق في الفصل الأول إلى تحليل الجوانب القانونية للجريمة المعلوماتية وأما الفصل الثاني فتناول فيه الجوانب القانونية للتحقيق وإجراءات جمع الدليل في الجريمة، حيث ساهم في إبراز جوانب مهمة من الموضوع تتعلق بتعريف الجريمة المعلوماتية وطبيعتها وأنواعها، كذلك الدوافع التي تقود لإرتكابها، مع التطرق إلى آليات التعاون الدولي الأمني والقضائي والجهود المبذولة في هذا الشأن، بالإضافة إلى مهام الأجهزة المختصة في عملية البحث والتحري والصعوبات التي تواجههم، حيث أفادتنا الدراسة في الاحاطة بالجانب القانوني للموضوع والإطلاع على أهم الإتفاقيات الدولية الموقعة، إلا أنها لم تخض في ميدان الأمن ونظرا لأن الدراسة تعود لسنوات مضت فلا تحتوي على القوانين الوطنية الحديثة وأهم الهيئات المستحدثة.

- دراسة لـ يوسف الصغير بعنوان "الجريمة المرتكبة عبر الانترنت":

مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزون، سنة 2013، حيث تناولت الدراسة الإجابة على الإشكالية التالية: خصوصية الجريمة الإلكترونية المرتكبة عبر الأنترنت مقارنة بالجرائم التقليدية والطرق الفعالة لمكافحتها؟ وعلى ضوء ذلك قسم البحث إلى فصلين تطرق في الفصل الأول إلى الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت والفصل الثاني تطرق إلى طرق مكافحة هذه الجريمة موضحا الطبيعة القانونية للجريمة وسمات المجرم الإلكتروني والقطاعات المستهدفة من قبله، وضحت لنا بشكل مفصل كل القوانين والتشريعات الوطنية الصادرة في هذا الشأن والمؤسسات المكلفة بمعالجة ومكافحة الجرائم الإلكترونية، ونظرا لأن الدراسة تعود إلى سنوات سابقة فإنها لا تحتوي على القوانين والتشريعات الحديثة والهيئات المستحدثة في هذا الشأن، كما يغيب الجانب الأمني في الدراسة.

- دراسة لـ يوسف بوغرارة بعنوان: "الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني":

مقال بمجلة الدراسات الإفريقية وحوض النيل، الصادرة عن المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، سبتمبر 2018، حيث حاول الباحث في هذه الدراسة الإجابة على الإشكالية الآتية:

إلى أي مدى إستطاعت الجزائر أن تحقق الأمن والدفاع السيبراني في الفضاء السيبراني؟ إنطلاقا من الفرضية الآتية: أدت الإصلاحات الجزائرية إلى تحقيق مستوى عالي من الأمن والدفاع السيبراني في الفضاء السيبراني، وقد تطرق الباحث في هذه الدراسة إلى الآليات القانونية والمؤسساتية لمكافحة الجريمة السيبرانية في الجزائر، وإستراتيجيات الدفاع وتحقيق الأمن السيبراني للجيش الوطني الشعبي، وفي الأخير اختتم الباحث هذا المقال بتقييم دور الجزائر في مجال الأمن السيبراني، وهذا ما جعلنا نفهم التوجهات الوطنية للأمن والدفاع وماهي الإستراتيجية المسطرة في ذلك، إلا أننا لاحظنا نقص في ذكر القوانين والتشريعيات الوطنية في هذا الشأن.

– دراسة لـ سمير بارة بعنوان: "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر – الدور والتحديات –":

مداخلة بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الإلتزامات السيادية والتحديات الإقليمية، جامعة قاصدي مرباح ورقلة يومي 30 و31 جانفي 2017. حيث عالج الباحث من خلال هذه الدراسة الإشكالية الآتية: ما هو دور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حالية ومستقبلا؟ حيث تم التطرق إلى النقاط الآتية: أساسيات عن الأمن السيبراني والجريمة السيبرانية، الدفاع الوطني وآليات تحقيق الأمن السيبراني، عوائق تحقيق الأمن السيبراني وفي الأخير أختتمت الدراسة ببعض التوصيات التي يتبناها المرصد العربي للسلامة والأمن في الفضاء السيبراني والتي أثرت دراستنا من خلال تناولها وضع إستراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، وكذلك الإلتزام بالقرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات ونشر ثقافة الأمن السيبراني، إلا أن الدراسة تخلو من القوانين الحديثة والهيئات المستحدثة نظرا لأن الدراسة تعود لسنة2017.

– دراسة لـ عنترة بن مرزوق، "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية":

مداخلة بالملتقى الدولي الثاني حول سياسات الدفاع الوطني بين الإلتزامات السيادية والتحديات الإقليمية، جامعة قاصدي مرباح ورقلة يومي 30 و31 جانفي 2017. حيث عالج الباحث من خلال هذه الدراسة مفهوم الأمن السيبراني، الإرهاب الإلكتروني كأحد أخطر التهديدات المحتملة على الأمن الجزائري في ظل الثورة التكنولوجية الحديثة، والجهود الجزائرية في مجال الأمن السيبراني، وفي الأخير أختتمت

المداخلة بمجموعة من التوصيات والتي أفادت موضوع دراستنا من جانب الأمن والدفاع السيبراني مثل: إقامة العدة العسكرية السيبرانية بتكليف عدد كبير من الأفراد العسكريين بمهمة القتال الافتراضي، تكوين نخب وطنية مختصة في مجال الأمن السيبراني، التعاون الإقليمي والدولي بتسيير تبادل المعلومات في مجال مكافحة الإرهاب الإلكتروني، منع تحول الفضاء السيبراني إلى فضاء للحروب والنزاع بين الدول إلا أن الدراسة لم تتناول القوانين والهيئات الحديثة نظرا لأنها تعود لسنة 2017 .

– دراسة لـ: نورة العقون، بعنوان: "واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر":

مذكرة تخرج مقدمة لإستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية شعبة العلوم السياسية، تخصص دراسات أمني واستراتيجية بجامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، سنة 2019/2018. حيث عالجت الطالبة من خلال هذه الدراسة الإشكالية التالية: كيف يؤثر الفضاء السيبراني على منظومة الدفاع الوطني في الجزائر؟ حيث تم التطرق الى النقاط التالية: تأثير الفضاء السيبراني على إستراتيجيات المنظومة الدفاعية في الجزائر مع التعرف على هذا الفضاء بمختلف خصائصه وكل ما ينتج عنه من تهديدات سيبرانية تمس بالأمن القومي الجزائري، مما فرض على الدولة الجزائرية تبني إستراتيجية خاصة لمواجهة هذه التهديدات، أين إستفدنا من الجانب الأمني في تناول الموضوع وهو ما لم تتطرق إليه الدراسات الأخرى، ما جعلنا نأخذ فكرة عن حجم التهديدات التي تتعرض له البلد، إلا أن الجانب القانوني لم يستوفى حقه من الدراسة.

بإطلاعنا على الموضوع تبين لنا أن هذه الدراسات تناولت تعريف الجريمة الإلكترونية وأنواعها وسمات مرتكبيها، بالإضافة إلى المجهودات الإقليمية والدولية التي توجت بالعديد من الإتفاقيات والمعاهدات والتوصيات الدولية لمكافحة الجرائم الإلكترونية، كما تناولت على الصعيد الوطني كل ما تم إنجازه من قبل الجزائر، فيما يخص القوانين والتشريعات المجرمة للجريمة الإلكترونية، كذلك المؤسسات والهيئات المكلفة بالتحقيق ومتابعة المجرمين على رأسهم الأجهزة الأمنية المتخصصة، كما تناولت الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني.

8- صعوبات الدراسة:

خلال دراستنا البحثية لهذه الظاهرة واجهتنا جملة من الصعوبات والعراقيل من بينها:

– الحالة الصحية للبلد وصعوبة البحث والتنقل (الحجر الصحي) بسبب تفشي فيروس كورونا كوفيد–19 حال دون إستغلال الكتب والمراجع على مستوى المكتبات الجامعية.

– عدم إجرائنا للدراسة الميدانية نظرا لحساسية الموضوع الذي يتميز بالسرية، الغموض والتكتم لدى المصالح الأمنية المختصة، التي ردت على طلبنا بالرفض.

– توفر المراجع باللغات الأجنبية، ما أدى إلى تعدد الترجمات والإختلاف في المصطلحات أمام كثرة المراجع والدراسات الأكاديمية التي تناولت الموضوع ضمن مقاربة قانونية أكثر منها مقاربة أمنية.

– تغير المشرف الأمر الذي حال دون إتمام دراستنا البحثية في وقتها المحدد وتضيع الوقت والجهد في الإجراءات الإدارية.

9- منهجية البحث:

من المعلوم أن كل دراسة أو بحث علمي يخضع لمنهج يتبعه الباحث خلال خطوات إنجازه لهذه الدراسة حتى يتمكن أن يعطي له صبغة وأساسا علميا وفي دراستنا هذه فإن طبيعة موضوع الدراسة يتطلب إتباع **المنهج الوصفي التحليلي** وذلك أن المنهج الوصفي يصف لنا الظاهرة محل الدراسة ومختلف الجوانب المحيطة بها والمنهج التحليلي من أجل تفسير وتحليل مختلف المؤشرات والإحصائيات المتعلقة بواقع الجرائم الإلكترونية.

كما تم الاعتماد على **الإقتراب القانوني المؤسساتي** من خلال تناول النصوص القانونية والمراسيم التنفيذية وتحديد عمل ومهام الهياكل التنظيمية والمؤسسات الرسمية.

10- خطة الدراسة:

قصد الإلمام بحيثيات موضع الدراسة تم إدراج مضامين وعرض محتوياته في ثلاثة فصول على النحو التالي:

لقد جاء الفصل الأول بعنوان **مقاربة معرفية حول الجريمة الإلكترونية** وذلك للتحكم في الأطر النظرية للظاهرة محل الدراسة وفهم كل الجوانب المحيطة بها.

فخصص **الفصل الأول** لعرض الجوانب المعرفية في الموضوع من خلال التطرق في المبحث الأول إلى ماهية الجريمة الإلكترونية وسمات مرتكبيها، والتطور الحاصل في مفهوم الأمن، وفي المبحث الثاني تم التطرق للفضاء السيبراني وإمتداداته وأبعاد الأمن السيبراني، أما المبحث الثالث تناول المجهود الدولي والإقليمي في مجال مكافحة الجريمة الإلكترونية من خلال إظهار أهم ما خلصت إليه المنظمات الدولية والإقليمية في مؤتمراتها وإتفاقياتها كالتشريع والتنسيق القضائي والأمني بين الدول.

كما جاء **الفصل الثاني** بعنوان "**السياسة الأمنية الجزائرية في محاربة الجريمة الإلكترونية**" وذلك بغرض التحكم في الأطر المؤسساتية والقانونية ومعرفة منظورها في التعاطي مع ظاهرة الدراسة، من خلال دراسة واقع الجريمة الإلكترونية في الجزائر ومدى توفر البنية المؤسساتية الأمنية لمحاربتها، حيث تناول المبحث الأول إحصائيات ومؤشرات وطنية ودولية عن واقع الجريمة الإلكترونية بالجزائر والإرهاب الإلكتروني، أما المبحث الثاني فقد تطرق إلى الآليات مكافحة الجريمة الإلكترونية من خلال القوانين والإتفاقيات الموقعة، مع التعريف بالبنية المؤسساتية الأمنية الجزائرية وكيفية عملها في إطار مكافحة الجرائم الإلكترونية على المستويين المحلي والدولي، ثم عالج المبحث الثالث التحديات وآفاق مكافحة الجريمة الإلكترونية بالجزائر من خلال ذكر التحديات والمعيقات التي تتعرض لها مختلف الأجهزة الأمنية أثناء أدائها لمهامها من ثم التطرق لمستقبل الأمن السيبراني في الجزائر في ظل التهديدات التكنولوجية الجديدة ومدى إستعداد الإستراتيجية الوطنية لمواكبة هذه المستجدات.

ثم جاء **الفصل الثالث** بعنوان "**دراسة ميدانية**" خصص للوقوف على حقيقة الظاهرة بفرقة مكافحة الجريمة المعلوماتية بأمن ولاية قالمة (المديرية العامة للأمن الوطني)، للتعرف على نوعية القضايا المعالجة والإحصائيات المسجلة، وطرق وأساليب عمل الفرقة المتخصصة، بالإضافة لآفاق التحديث وسبل العصرنة على ضوء توجهات المنظومة الأمنية الوطنية، إلا أني لم أستطيع إنجاز الدراسة، حيث لقي طلبي تحفظا من قبل السيد/ مدير أمن ولاية قالمة، نظرا لخصوصية العمل الأمني وطابع السرية الذي يميزه.

وتختتم هذه الدراسة بخاتمة عامة، نستعرض فيها أبرز النتائج المتوصل إليها بالإضافة إلى جملة من المقترحات.

الفصل الأول:
مقاربة معرفية حول الجريمة الالكترونية

تمهيد:

يشهد العالم تحديات كبيرة ومتزايدة، نتيجة التطورات السريعة التي وصلت إليها تكنولوجيا الإتصال والمعلومات والتي إستغلها المجرمون في إلحاق الضرر بالأفراد والمجتمع من خلال الشبكة العنكبوتية؛ ما جعلهم مخالفين للقانون ومحل العديد من المتابعات القضائية.

فالجريمة الإلكترونية تختلف عن غيرها من الجرائم بالنظر لطبيعتها وخصوصيتها، هذا ما جعل الباحثين والعلماء يعيدون النظر في نوعية التهديدات والمخاطر التي أصبح الفضاء السيبيراني مصدرا لها خاصة أمام تنوع أشكال الجريمة الإلكترونية وأخص هنا بالذكر الإرهاب الإلكتروني وبالتالي كان لا بد من إعادة النظر في مفهوم الأمن الكلاسيكي، حيث فرض الواقع التعاون الدولي أولوية الدول في مكافحة الجرائم الإلكترونية.

ومن أجل توضيح ذلك قمنا بتقسيم الفصل الأول إلى ثلاثة مباحث التالية:

المبحث الأول: الجريمة الإلكترونية على ضوء الإشكآليات الجديدة للأمن.

المبحث الثاني: الفضاء السيبراني ومجالات إنتشار الجريمة الإلكترونية.

المبحث الثالث: أشكال التعاون الدولي لمواجهة الجريمة الإلكترونية.

المبحث الأول: الجريمة الإلكترونية على ضوء الاشكآليات الجديدة للأمن.

الجريمة الإلكترونية من الجرائم الحديثة المهددة للأمن، التي يعد تحديد مفهومها الخطوة الأولى لتعرف على هذه الظاهرة من جميع جوانبها، وهذا ما يحيلنا الى فهم ومعرفة الأسباب التي أثرت على تطور مفهوم الأمن التقليدي.

المطلب الأول: سياقات ضبط مفهوم الجريمة الإلكترونية.

أثار الفقهاء العديد من التساؤلات وطرحوا الكثير من الآراء، حول تعريف ظاهرة الجريمة الإلكترونية، نظرا لما تتميز به عن غيرها من الجرائم المستحدثة، حيثبذل الفقهاء المجهود الكثير محاولين فهم المقصود بالجريمة الإلكترونية، وتحديد تعريف مجمع لها مع تبين طبيعتها القانونية، كما أن تعريفها يستوجب الإلمام بالجانب الموضوعي والإجرائي، مع دراسة العوامل التي تتداخل في تكوينها، والإحاطة بمختلفة الأمور الفنية المتعلقة بها.

وعليه سنتطرق إلى ماهية الجريمة الإلكترونية، ومختلف التعريفات التي أستخدمت لوصفها، مع توضيح المعايير التي إستند عليها الفقهاء في تعريفهم لها، ولا يكتمل البحث في هذه الظاهرة، دون البحث في نشأتها وخصائصها ودوافع إرتكابها وسمات مرتكبيها، وهو ما سنتطرق إليه في هذا المطلب.

1- نشأة الجريمة الإلكترونية:

يرجع أول ظهور للجريمة الإلكترونية إلى العقد الثامن من القرن العشرين، حيث نشر المركز الوطني للبيانات الأمريكي تقريرا حول الجرائم الإلكترونية، والتي كانت لا تتعدى سرقات برامج الكمبيوتر وإتلاف تلك البرامج؛ ويمكن القول أن جرائم الحاسوب ترجع لعام 1960، أما جرائم شبكة الأنترنت فأنها بدأت بإكتشاف العدوان الفيروسي الذي عرف في التاريخ القانوني بجريمة " دودة موريس"عام 1988.[1]

كما أقدمطالب دكتوراه أمريكي في السنةنفسها،بوضع برنامج على الحاسوب مرتبط بشبكة الأنترنت واخترق به الجدار الأمني،من أجلإثباتعدم فاعلية النظم الأمنية المستخدمة في حماية الحاسب الآلي،ورغم نجاح برنامجه وإنتشاره بشكل واسع بين أجهزة الكمبيوتر الحكومية، إلا أنه تسببخسائر مادية

[1]عبد العال الديربي ومحمد صادق إسماعيل: **"الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت"**. ط1، المركز القومي للإصدارات القانونية، مصر،2012 ، ص23.

و تعطيل العديد من مصالح الدولة، ورغم عدم تعمده إحداث أي ضرر، إلا أنه وقع في الدخول الغير المشروع ،وتمت ادانته بالوضع تحت المراقبة لفترة وغرامة مالية تقدر بـ 10 آلاف دولار.[1]

ومع التطور العلمي و زيادة الجريمة الإلكترونية، صاحب تلك الزيادة إرتفاع في معدل الجرائم التي تستخدم فيها الأنترنت، نذكر منها بعض الحالات كاختراق القراصنة الروس للمؤسسات الأمريكية وسرقة بعض المعلومات الحساسة من الجهات العسكرية، و كذلك الهجوم على شبكة الفضاء الأمريكية ناسا NASA، واقتحام المنتدى الإقتصادي العالمي بدافوس " بسويسرا "،بهدف سرقة معلومات عن شخصيات حساسة تتعلق ببطاقات الإئتمان[2] ولعل ذلك يبين أن الاستخدام الإجرامي لشبكة الأنترنت لا يقل خطورة على الإجرام التقليدي.

2- تعريف الجريمة الإلكترونية:

رغم اجتهاد الفقهاء في وضع تعريفات للدلالة على مفهوم الجريمة الإلكترونية، إلا أننا لم نجد مصطلحا واحدا جامعا لهذه الظاهرة، والتي تستعمل تكنولوجيا الإتصال والمعلومات لإرتكابها؛ نظرا لوجود هذا الفراغ القانوني، وضع الفقه عدة تعريفات لها ، حيث انقسمت بدورها إلى اتجاهين رئيسيين وهذا بالنظر إلى الزاوية التي ينظر منها لهذا النوع من الجرائم، حيث أن الاتجاه الأول مضيق لمفهوم الجريمة الإلكترونية، أما الاتجاه الثاني فقد حاول التوسع في تعريفه.

❖ التعريف لغوي:

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه وجريمة الرجل على قومه وإليهم: أذنب وجنى جناية.[3]

---

[1] عبد العال الديربي ومحمد صادق إسماعيل، المرجع السابق، ص 23.

[2] نابر نبيل عمر: **"الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية دراسة في المحل الإلكتروني المسوغ بالحماية القانونية وبحث المفردات المشمولة بالرعاية وآلية التطبيق في القانون المصري والمقارن"**. رسالة مقدمة لنيل شهادة ماجستير في الحقوق، جامعة الإسكندرية، كلية الحقوق، دار الجامعة الجديدة، 2012، ص 13-14.

[3] فاطمة الزهرة بختي: **"إجراءات التحقيق في الجريمة الإلكترونية"**. مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014/2013 ، ص 09.

❖ **التعريف الاصطلاحي:**

عرفها المأوردي في الأحكام السلطانية بقوله " **الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير يعني إذا كانت ممن يتعمد إرتكابها**"، كما عرفها الإمام أبو زهرة قائلا: **"هي المعصية التي يكون فيها عقاب يقرره القضاء".**[1]

أ. المفهوم الضيق للجريمة الإلكترونية:

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية، وأن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية.

من التعريفات التي وضعها أنصار هذا الاتجاه أيضا ما ذهب إليه الفقيه ميرفي سيرن Merve Seren حيث يرى أن الجريمة الإلكترونية: "**هي الفعل غير المشروع الذي يدخل في إرتكابه الحاسب الآلي أو هي الفعل الإجرامي الذي يستخدم في إرتكابه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات**".[2]

فيما ذهب الفقيه روجر **روسنبلات** Rojer Rosenblatt على أنها: "**كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تغييرها أو حذفها أو التي تحول عن طريقه**".[3]

حسب الدكتورة هدى فشقوش هي: ""**كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، أو هي أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات**".[4]

---

[1] فاطمة الزهرة بختي، نفس المرجع السابق، ص 09.

[2] طارق إبراهيم الدسوقي عطية: **"الأمن المعلوماتي النظام القانوني للحماية المعلوماتية"**. دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص 153.

[3] فريال لعقال: **"الجريمة المعلوماتية في ظل التشريع الجزائري"**. مذكرة لنيل شهادة الماستر في القانون العام، جامعة أكلي محند أولحاج البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، سنة 2014-2015، ص9.

[4] خالد عباد الحلبي: **"إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت"**. ط1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص28.

عرفها كل من CASTLET TOTT و A. HARD بأنها: **"تلك الجرائم التي يكون قد حدث في مراحل إرتكابها بعض العمليات الفعلية داخل الحاسوب، وبمعنى آخر هي التي يكون للحاسب الآلي فيها دورا إيجابيا أكثر من سلبيته"**[1].

يؤخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بمختلف جوانب الظاهرة، كون بعض الفقهاء ذهب في اتجاه التركز على معيار موضوع الجريمة، والبعض الآخر ركز على وسيلة إرتكابها، وآخرون على النتيجة كمعيار.

ب. المفهوم الواسع للجريمة الإلكترونية:

إزاء الانتقادات التي وجهت الى الاتجاه الأول، حاول الفقهاء تعريف الجريمة الإلكترونية على نحو واسع، لتفادي القصور الذي شابت تعريفات الاتجاه المضيق.

وعلى العكس من الاتجاه السابق، فان أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة الإلكترونية، حيث يرى الفقيهان MICEL,CREDO بأنها كل جريمة يستخدم فيها الكمبيوتر كوسيلة من أجل الدخول الغير مصرح به، لحاسوب وبيانات المجني عليه.[2]

تناول رأي آخر تعريفها على أنها: "كل فعل يرتكب من قبل أي شخص يهدف إلى إلحاق ضرر بشبكة الأنترانت أو بيانات الكمبيوتر، ومجرم في قانون العقوبات.[3]

كما تشمل هذه الجريمة الإعتداء المادي على أجهزة الكمبيوتر وملحقاته أو سرقتها والاستخدام الغير شرعي للبطاقات الإئتمانية، والإختراق الإلكتروني للموزعات والحاسبات الآلية، وتزييف المكونات المادية والمعنوية للكمبيوتر.[4]

---

[1] أحمد خليفة الملط: **"الجرائم المعلوماتية"**. ط2، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 30.

[2] محمد على العريان: "**الجرائم المعلوماتية**"، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004، ص ص44، 45.

[3] طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 158.

[4] المرجع نفسه، ص ص44، 45.

عرفت في **إطار المنظمة الأوربية للتعاون والتنمية الإقتصادية** بأنها: "كل فعل أو إمتناع من شأنه أن يؤدي إلى الإعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية.[1]

كما عرفها **مكتب تقيم التقنية في الولايات المتحدة الأمريكية** بأنها: "الجرائم التي تلعب فيها ببيانات الكومبيوتر والبرامج المعلوماتية".[2]

وجاء في توصيات **مؤتمر الأمم المتحدة العاشر** لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا سنة 2000 على أنها كل جريمة تكون وسيلة إرتكابها الشبكة الحاسوبية أو الحاسوب الذي يمكن أن تقع بداخله الجريمة.[3]

إن هذا الاتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية، إذ يمكن أن تدخل في دائرته العديد من الجرائم الأخرى، والتي لها وصف جزائي مغاير تماماالهذه الظاهرة، حتى لو إستعمل المجرم الحاسوب الآلي في النشاط الإجرامي، فإن بعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا لا يمكن اعتبارها جريمة إلكترونية لمجرد أن الحاسوب أو أحد لواحقه المادية كانت محلا لفعل السرقـة.

جـ. تعريف المشرع الجزائري للجريمة الإلكترونية:

عرف المشرع الجزائري الجرائم الإلكترونية في المادة 02 من قانون 04/09 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن منظومة معلومات أو نظام الإتصالات الإلكترونية".[4]

على ضوء ما سبق ذكره من أراء، وعدم الاتفاق على تعريف اصطلاحي جامع، يمكن أن نستنتج أن الجريمة الإلكترونية هي كل فعل يتم التخطيط له بإستعمال أي نوع من الحواسيب الآلية سواء حاسب شخصي أو شبكات الحاسب الآلي أو وسائل التواصل الإجتماعي لتسهيل إرتكاب جريمة أو عمل مخالف

---

[1] فريال لعقال: مرجع سابق، ص 11.

[2] ريم عميار: " **تأثير الجريمة المعلوماتية على الاقتصاد الوطني**"، مذكرة لنيل شهادة الماستر في القانون العام، جامعة العربي بن مهيدي أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2017-2018، ص9.

[3] حنان ريحان مبارك المضحاكي، مرجع سابق، ص ص 26، 27.

[4] القانون04.09 المؤرخ في 05 أوت2009، يتضمن " **القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والإتصال ومكافحتها**" الجريدة الرسمية، العدد47 المؤرخ في 05 أوت 2009 ص6.

للقانون، كما تعتبر كل عملية إختراق عبر شبكة الأنترنت للبيانات الشخصية والحكومية قصد إتلافها أو تعطيلها جريمة إلكترونية.

3- خصائص الجريمة الإلكترونية:

تختلف الجرائم الإلكترونية عن غيرها من الجرائم التقليدية، نظرا لطبيعتها وطريقة إرتكابها، مما جعلها تتميز بالخصائص التالية:

- **صعوبة إكتشاف الجريمة الإلكترونية:** تتميز بأنها صعبة الإكتشاف ذلك أنها تتم في الخفاء وليست ظاهرة أو ملموسة، كما أن المجرم لا يترك ورائه أي دليل مادي لإدانته، بسبب قدرته على محو الاثار اثبات الجريمة في أقل من ثانية واحدة، وهذا ما يصعب عملية الوصول إليه وإدانته.
- **الجرائم ترتكب عبر شبكة الأنترنت:** تعد شبكة الأنترنت هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها والتي تكون غالبا ضحية لتلك الجرائم وهو ما دعها إلى اللجوء إلى نظم الأمن الإلكترونية في محاولة منها لتحمي نفسها أو على الأقل لتقلل من خسائرها عند وقوعها ضحية لتلك الجرائم.[1]
- **الكمبيوتر وسيلة إرتكاب الجريمة الإلكترونية:** إن لكل جريمة أداة يعهد لها المجرم لتنفيذ جريمته ويعتبر الحاسب الآلي في الجرائم الإلكترونية الأداة والوسيلة التي ينفذ من خلالها المجرم إلى شبكة الأنترنت من أجل إرتكاب جرائمه مهما كانت نوعيتها وجسمتها.
- **مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسب الآلي:** يتميز مرتكب الجريمة الإلكترونية بخبرته الواسعة في التحكم في الحاسب الآلي وبرامجه المختلفة التي تمكنه من ولوج شبكة الأنترنت وإرتكاب جريمته دون أن يتم إكتشافه، مستعينا بذلك بخبرته في عدم كشف هويته أو الوصول لأدلة ضده.[2]

---

[1] عبد الحكيم مولاي إبراهيم: "**الجرائم الإلكترونية**"، مجلة الحقوق والعلوم الانسانية، العدد23، جامعة زيان عاشور بالجلفة، الجزائر، سنة 2015، ص 213.

[2] منير محمد الجنبيهي وممدوح محمد الجنبيهي: "**جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها**"، دط، دار الفكر الجامعي، الإسكندرية، 2004، ص ص 14، 15.

- **جريمة عابرة للحدود:** بفعل التطور شبكة الأنترنت لم تعد هناك حدود مادية تعيق عملية تحويل البيانات بين دول وهذا يعتمد على قدرة الحواسيب والشبكات في تبادل ونقل المعطيات إلى أنظمة دول أخرى بعيدة ألاف الأميال، وهذا يجعلها تتأثر بالجريمة الإلكترونية في ان واحد.[1]

4- دوافع إرتكاب الجرائم الإلكترونية:

الدافع (الباعث) أو الغرض، الغاية، كلها تعبيرات لها دلالتها الإصطلاحية في القانون الجنائي تتصل بما يعرف بالقصد الخاص بالجريمة[2]، والدافع هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي، حيث أن للجريمة الإلكترونية عدة دوافع ساهمت في إرتكابها وإنتشارها، يمكن أن نذكرها فيما يلي:

- **الدوافع المادية:** نتيجة للعائدات المالية التي يجنيها المجرم من خلال التزوير والتلاعب فأنها تشكل حافزا قويا لأصحاب النوايا السيئة في إرتكاب جريمتهم في استبيان أجراه أحد الباحثين في أمريكا عام 1995 بين أن معدل أرباح مرتكب جريمة الحاسوب وصلت إلى "600,000" دولار مقابل 300,000 دولار لمرتكب الجريمة في النظام اليدوي.[3]
- **الدوافع الشخصية:** غالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة إحساسه بالقوة والذات وبقدرته على اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات ومن أجل تأكيد قدرته الفنية على إرتكاب أحد جرائم الكمبيوتر وقد يكون الهدف من إرتكاب الجريمة الحقد والكراهية.
- **الدوافع الذهنية أو النمطية:** الصورة الذهنية لمرتكبي جرائم الحاسب الآلي والأنترنت غالبا هي صورة البطل والذكي الذي يستحق الإعجاب، لا صورة المجرم الذي يستوجب محاكمته فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى براعتهم.[4]

---

[1] Mascalacorinne. « Criminalité et contrat électronique » travaux de l'association, CAPITANT. henir journées national .paris 2000. p119

[2] نجيب حسني: "**دروس في القانون الدولي الجنائي**"، القاهرة، د.ط، دار النهضة العربية، 1960، ص 152.

[3] عبد العال الديربي ومحمد صادق إسماعيل، مرجع سابق، ص 51-52.

[4] نسرين عبد الحميد نبيه: "**الجريمة المعلوماتية والمجرم المعلوماتي**"، د.ط، منشأة المعارف، الأردن، د.ت، ص ص44، 45.

- **الفرص المتزايدة:** أن ازدياد عدد مستخدمي الحاسوب من ذوي المعرفة والمقدرة في اختراق البيانات نتيجة "لا مركزية المعالجة"، الشبكات الإتصالات والدخول عن بعد إلى الحاسوب قد اتخذت فرصا متزايدة للمزورين والمتلاعبين لتنفيذ أغراضهم لاسيما في ظل سيطرة ورقابة غيركفئة في هذا المحيط الإلكتروني لمعالجة البيانات.
- **صعوبة الإكتشاف:** نظرا لكثرت البيانات المخزنة في الحاسوب يجعل من أي تزوير أوتلاعب عملية سهلة، خاصة إذا تمكن المجرم من عدم ترك أي دليل خلفه، وهو الأمر الذي يجعلعملية إكتشاف الجريمة صعبة للغاية.

وهذا ما ذهب إليه "دوغلاس بيرت"، أحد المسؤولين في مركز الحماية من جرائم الحاسب الآلي التابع للشرطة الفيدرالية الأمريكية بأنه: "**لا يمكننا أن نتوقع كل شيء لأن تحديد الخطر أمر بالغ الصعوبة**".[1]

- **حب المغامرة والإثارة:** جاء على لسان أحد القراصنة في كتاب أنظمة الكمبيوتر، أنه كانت القرصنة هي النداء الأخير الذي يبعثه دماغي.[2]
- صعوبة الإحتفاظ بأثارها أن وجدت.
- تحتاج إلى خبرة فنية وتقنية ويصعب على المحقق التقليدي التعامل معها.
- تعتمد على الخداع في إرتكابها والتضليل في التعرف على مرتكبيها.
- تعتمد على قمة الذكاء والمهارة في إرتكابها.
- الولع في جمع المعلومات وتعلمها.[3]

---

[1] عبد الحكيم رشيد توبة: "**جرائم تكنولوجيا المعلومات**"، ط1، دار المستقبل، عمان، 2008، ص52.

[2] منال مباركي: "**أشكال الجريمة الإلكترونية المرتكبة عبر الفايسبوك**". دراسة ميدانية على عينة من الشباب المستخدمين للموقع في الجزائر، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والإتصال تخصص اتصال وعلاقات عامة، جامعة العربي بن مهيدي أم البواقي، كلية العلوم الإنسانية والإجتماعية، قسم العلوم الإنسانية، 2017/2016، ص68.

[3] منال مباركي، نفس المرجع السابق، ص 69.

5- سمات مرتكب الجريمة الإلكترونية:

إن الخصائص التيميزت الجريمة الإلكترونية عن غيرها من الجرائم يدل على أن الشخص المرتكب لهذه الجريمةمتميز عن باقي المجرمين، كونه يتفرد بجملة منالسمات لا تجدها إلا في المجرم الإلكتروني، نذكر منها ما يلي:

- **التخصص:** يعني أن المجرم متخصص في جرائم الحاسب الآلي والأنترنت ولا تجده يهتم بالتورط في الجرائم التقليدية الأخرى، كونه متخصص في هذا النوع من الإجرام.[1]
- **الذكاء والاحتراف:** يتمتع المجرم الإلكتروني باحترافية عالية في تنفيذ جرائمه، وذلك لإكتسابها لمهارات التقنية الخاصة بالحاسب الآلي والأنترنت، بل هنالك من المجرمينهم أنفسهمأصحاب الاختصاص في معالجة المعلومات آليا، كما أن جرائم السرقة والنصب وغيرها، تتطلب دراية واسعة بتكنولوجيا المعلوماتية.[2]
- **الخبرة والمهارة:** يتسم مرتكب الجريمة الإلكترونية بأنه على درجة عالية من الخبرةوالمهارة في استخدام التقنية المعلوماتية، وهذا ما يأهله لابتكار أساليب وطرق متميزةيرتكب بهاجرائمه [3]
- **الميل إلى إرتكاب الجريمة:** وهي النزعة التي تميزه عن غيره من الأشخاصوتجعله يستغلمؤهلاته العلمية والتقنية في مجال تكنولوجيا المعلوماتية، كي تساعده على إرتكاب الجرائم.[4]
- **شخصية مثابرة وصبورة:** ليس من السهل إرتكاب الجرائم الإلكترونية، ما لم يتحلى المجرم بقوة التحمل والمثابرة، فالإختراق إلكتروني أو تحويل الأموال يستغرق منه وقتا طويلا، قد يأخذ ساعات أو أيامفي تكرار المحاولات قصد تحقيق أهدافه الإجرامية.[5]

---

[1] نهلا عبد القادر المومني: مرجع سابق، ص 55.

[2] أيمن عبد الحفيظ: "الإتجاهات **الفنية والأمنية لمواجهة الجرائم المعلوماتية**"، د.ط، دون دار نشر، دون بلد نشر، 2005، ص13.

[3] يوسف جفال: "**التحقيق في الجريمة الإلكترونية**"، مذكرة لنيل شهادة الماستر في القانون الجنائي، جامعة محمد بوضياف المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2017/2016، ص 14.

[4] أيمن عبد الحفيظ، مرجع سابق، ص 15.

[5] ربيعي حسين: "المجرم المعلوماتي شخصيته وأصنافه". **مجلة العلوم الإنسانية**، العدد 40، جامعة محمد خيضر، بسكرة، جوان2015، ص290.

المطلب الثاني: الأمن والتهديدات والمخاطر الجديدة.

لقد أصبح اليوم الأمن يعني أكثر ضمان إستقرار الدولة والحفاظ على السلم الإجتماعي وحماية أمن الأفراد من التأثيرات السلبية للعولمة ، التي مست كل الميادين ذات الصلة بالنشاط الإنساني، أدت بذلك هذه النظرة الجديدة للواقع الأمني إلى إعادة النظر في مفهوم الأمن وعدم حصره في الميدان العسكري.

1- مفهوم الأمن:

أ- التعريف اللغوي:

يعرف الأمن في اللغة العربية عن المصدر أمن ، يأمن ، أمان ، آمنه ،أطمأن ولم يخف فالأمن عكس الخوف ويقصد به السلامة فسلم البلاد أي أمن سكأنه وأطمأن أهله فيه واستقروا به سلام دون خوف.[1] ويعرفه قاموس محيط المحيط العربي " الأمن ضد الخوف مطلقا أي سواء كان من العدو أو غيره أو عدم توقع مكره في الزمان الآتي".[2]

أما في اللغة الانجليزية عرف الأمن Security قاموس أكسفورد " أنه حالة التحرر من الخطر والخوف، فهو أمن الدولة والمنظمات من النشاطات الإجرامية كالإرهاب واللصوص والجواسيس"[3]وجاء تعريفه في قاموس كامبريدج على أنه " حماية الأشخاص والبنايات"، كما عرفه قاموس Larousse الفرنسي " بأنه غياب أو التخفي من المخاطر في مجال معين".[4]

---

[1] العايب أحسن: **" الأمن العربي بين متطلبات الدولة القطرية ومصالح الدول الكبرى 1945-2006"**، أطروحة لنيل درجة الدكتورة في العلوم السياسية، جامعة الجزائر3، كلية العلوم السياسية والاعلام، قسم العلوم السياسية والعلاقات الدولية، سنة 2008، ص13.

[2] المعلم بطرس البستاني، محيط المحيط: **قاموس مطول للغة العربية**، مكتبة رياض الفتح: بيروت، سنة 1987، ص 08

[3] Oxford university press; Oxford word power. (New York :database right oxford university press. 2016) P693.

[4] http://www.larousse.fe/dictionnaires/francais/s /s%C3%A9curit%C3%A9/71792

تعرف دائرة المعارف البريطانية الأمن " على أنه حماية الأمة من خطر القهر على يد قوة أجنبية " وهو حالة تصبح الدولة بمنأى عن أي تهديد سواء عسكري، سياسي، اقتصادي...إلخ ما يجعلها تملك استقلالية في اتخاذ قراراتها من أجل تحقيق التنمية.[1] .

أما هنري كيسنجر وزير الخارجية الأسبق للولايات المتحدة فيعرفه "على أنه جميع الإجراءات المتخذة من قبل المجتمع بغرض الحفاظ على حقه في البقاء"، كما أن روبرت مكنمارا وزير الدفاع الأمريكي الأسبق وأحد مفكري الإستراتيجية البارزين يرى في كتابه "**جوهر الأمن**" أن الأمن يعني التطور والتنمية الإقتصادية، الإجتماعية، السياسية في ظل حماية مضمونه" وهذا يعني أنه ينظر إلى الأمن على أنه تقوية الدولة لنفسها اعتمادا على مقدراتها وإمكانيتها التي توفر لها سبل التنمية وهذا لا يتحقق إلا بحماية هذه الإمكانيات من أي خطر أو تهديد.[2]

وذهب كذلك بطرس بطرس غالي الأمين العام السابق للأمم المتحدة إلى القول "أن الامن لا يقتصر على التهديد العسكري الخارجي فقط أو سلامة الدولة وسيادتها ووحدتها الإقليمية، إنما يشمل الإستقرار السياسي والإقتصادي والإجتماعي".[3]

إلا أن باري بوزان Barry Buzan المختص في الدراسات الأمنية يرى أنه "في حالة الأمن يكون النقاش دائر على السعي للتحرر من التهديد، أما إذا كان هذا النقاش في إطار النظام الدولي، فإن الأمن يتعلق بقدرة الدول والمجتمعات على صون هويتها المستقلة وتمسكها العملي" ويقصد بذلك أن الأمن يتطلب العمل على التحرر من التهديدات وتمسك بالقيم الوطنية وإستقلاليتها في سياق النظام الدولي".[4]

وعلى ضوء التعريفات السابقة يمكننا ان نعرف الأمن" **أنه القدرة التي تتمكن بها الدولة من تأمين مصادر قوتها الداخلية والخارجية، الإقتصادية والعسكرية في شتَّي المجالات ومواجهة المصادر التي تهدِّدُها في السلم والحرب، مع استمرارية ضمان توفر تلك القوى في الحاضر والمستقبل**".

---

[1] عبد الحميد عائشة وملوك نوال، "الإجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر"، **مجلة المفكر للدراسات القانونية والسياسية:** المجلد 3، العدد 3، الجزائر، سبتمبر 2020، ص213.

[2] روبرت ماكنمارا، **جوهر الأمن**، ترجمة، يونس شاهين، القاهرة: الهيئة المصرية العامة للنشر، 1971، ص 39.

[3] بن عنتر بوزنادة ،" تطور مفهوم الأمن في العلاقات الدولية"، **السياسة الدولية**، العدد 160، أفريل 2005، ص57.

[4] نعيمة خطير ، "الأمن كمفهوم مطاطي في العلاقات الدولية ...إشكالية التوظيف والتعريف "، **المجلة الجزائرية للأبحاث والدراسات**، المجلد 1، العدد 2، جامعة جيجل، الجزائر، 2018، ص244.

2- ظهور منظومة مفاهمية جديدة:

لقد عرفت الحرب الباردة تنافسا عسكريا بين الولايات المتحدة الامريكية والإتحاد السوفياتي، غلبت عليه المسائل الأمنية وفق آلية ميزان القوة والتحالفات والردع النووي، وبعد نهايته تحول الصراع إلى داخل الدول بعد أن كان خارجها، ما فرض عليها التعاطي مع هذه التهديدات الداخلية والمتمثلة في تعدد العرقيات، الديانات، الجماعات السياسية الإثنية المدفوعة بالرغبة في الإنتقام، يضاف إليها جملة من الاثار السلبية التي أثارتها العولمة لهذه النزاعات الداخلية.[1] وهذا ما يضعف الدول ويجعلها غير قادرة على تنمية قدراتها الإقتصادية والعلمية والعسكرية وتصبح غير أمنة معرضة لشتى أنواع المخاطر.

حيث أن الصراع التقليدي أصبح اليوم إلكتروني، يعكس طبيعة النزاعات التي تحدث بين الدول على أساس خلفيات قد تكون دينية أو عرقية أو إقتصادية أو سياسية...إلخ، وهذا الصراع تمدد داخل شبكات الإتصال والمعلوماتية، متحديا الحدود الاقليمية للدول وسيادتها، واضافت عملية تعدد الاستخدامات والفاعلين والمصالح من تنوع أشكاله وأهدافه، خاصة أمام تأثيراته النفسية والمعنوية والاعلامية التي تصبح أمنية وعسكرية، وهي بذلك تعد جبهة من جبهات القتال الإلكتروني.[2]

وهناك أربعة مستويات للأمن يمكن ذكرها كما يلي:[3]

أ) **أمن الفرد:** هو أي خطر يهدد حياة الفرد وما يمتلكه.

ب) **أمن الوطن:** هو كل تهديد يأتي من داخل التراب الوطني أو خارجه.

ج) **الأمن القطري أو الجماعي:** أي تهديد يهدد إقليم معين والذي تتفق مجموعة من الدول على مواجهته.

د) **الأمن الدولي:** يتعلق بأمن دول العالم والذي يتولاه المنظمات الدولية كالأمم المتحدة أو مجلس الأمن الدولي من أجل الحفاظ على السلم والأمن الدوليين.

---

[1] السيد السليم: **"تطور السياسة الدولية في القرن التاسع عشر والقرن العشرين"**. د.ط، دار الفجر للنشر والتوزيع، القاهرة، 2002.

[2] نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني- التهديدات المتصاعدة لأمن الدول-"، **مجلة مركز بابل الانسانية**، المجلد08، العدد02، 2018، ص193

[3] عائشة عبد الحميد و نوال ملوك، مرجع سابق، ص 213.

3 – التهديدات والمخاطر الجديدة:

لقد أصبحت الجرائم الإلكترونية مصدر تهديد حقيقي لإقتصاديات الدول ولم تعد تقتصر على جرائم سرقة أموال البنوك والأفراد بل تعدى الأمر إلى مهاجمة قطاعات إستراتيجية على غرار أمن الموانئ، حيث أصبح المجرمون يجنون أرباحا تفوق تلك التي يحصلون عليها من تجارة المخدرات، فإذا أخذنا دولة الامارات على سبيل المثال فإننا نجدها منذ 2014-2015 يوجد بها حوالي مليوني شخص ضحية الجرائم الإلكترونية، كما يلاحظ إرتفاع الجريمة الإلكترونية في الوطن العربي إلى نحو 26 مليون عملية قرصنة، كما سجلت الجزائر سنة 2016 حسب مصدر موثوق لجريدة الفجر 500 جريمة إلكترونية معظمها تتعلق بعملية السطو على الصور والبيانات الشخصية، الإعتداء على الأنظمة المعلوماتية.[1]

كما أن أحداث 11 سبتمبر 2001 تعد مفصلية كونها بداية ظهور الإرهاب الإلكتروني وإستعماله لشبكة الأنترنت بشكل بارز في الترويج لفكره المتطرف، أين أصبح الفضاء الإلكتروني ساحة قتال وصراع بين تنظيم القاعدة والولايات المتحدة الأمريكية ، ولم يتوقف ذلك بل حدثت سنة 2007 عمليات عدائية بين كل من روسيا وإستونيا، لتعاد المواجهات الإلكترونية مرة أخرى بين روسيا وجورجيا سنة 2008 ، وهذا دون أن ننس مع تعرض له البرنامج النووي الايراني سنة 2012 اثر الهجوم الإلكتروني باستخدام فيروس "ستاكسنت" [2] أنّ كل هذه الاحداث تظهر مدى التحول الجديد في طبيعة الصراعات والتهديدات التي تهدد الأمن الوطني والدولي على حد سواء.

---

[1] نورة شلوش، مرجع سابق، ص 201.

[2] اسماعيل زروقة: "الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، **مجلة العلوم القانونية والسياسية**، المجلد10، العدد01، أفريل 2019، ص1020.

المبحث الثاني: الفضاء السيبراني ومجالات إنتشار الجريمة الإلكترونية

لقد أصبح الفضاء السيبراني يأخذ حيزا كبيرا ضمن إستراتيجيات الدفاع للدول كونه مصدر للتهديدات المختلفة والتي تأثر على الأمن السيبراني لهذه الأخيرة بجميع أبعاده ومن بين هذه التهديدات الهجمات السيبرانية، الجريمة الإلكترونية بأنواعها والتي تتسبب بخسائر مادية ومعنوية لأفراد ومؤسسات الدولة المستهدفة.

المطلب الأول: مفهوم وامتدادات الفضاء السيبراني.

أولا: الفضاء السيبراني:

1- تعريف الفضاء السيبراني:

هناك من عرفه على: بأنه عالم افتراضي يتداخل مع عالمنا المادي ، يتأثر به ويؤثر فيه بشكل معقد حيث تربطهما علاقة تكاملية تحمل العديد من المزايا والمخاطر، هناك من وصفه بالذراع الرابعة للجيوش الحديثة إلى جوار القوات الجوية والبحرية والبرية، خاصة أن معارك حقيقية أصبحت تدور أحداثها داخلهذا الفضاء الافتراضي.[1]

وهناك من يرى أنه يمثل البعد الخامس للحرب، كما يعرف على أنه: المجال المادي والغير المادي الذي يتكون من عناصر هي أجهزة الكومبيوتر، والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد كل هذه العناصر العامل المشترك في جميع محأور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمتها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متآخرة.[2]

---

[1] عباس بدارن: **"الحرب الإلكترونية، الاشتباك في عالم المعلومات"**. بيروت، مركز دراسات الحكومة الإلكترونية، 2010، ص4.

[2] يائير كوهين: **"الفضاء الإلكتروني والبعد الخامس للحرب"**. محاضرة في المؤتمر الـ 16 لرابطة الأنترنت الإسرائيلية، مدينة القدس، 2012، ص 22.

2- خصائص الفضاء السيبراني:

ينفرد الفضاء السيبراني بمجموعة من الخصائص التي تميزه عن البر، البحر، الجو والفضاء ويمكن إجمال هذه الخصائص فيما يلي:[1]

- الفضاء السيبراني يعتمد على المجال الكهرو مغناطيسي، والذي يعطي لتكنولوجيا المعلومات والإتصالات (HCT) القدرة على العمل.
- انعدام الخيارات في الفضاء السيبراني على عكس الجو، البحر، البر، الفضاء والذي يوجد فيه ميدان واحد، ففي ميدان الجو مثلا يحسم الأمر بتدمير طائرة العدو، في حين أن في الفضاء السيبراني عندما تقوم بإغلاق موقع إلكتروني ما، فإن عملية إسترجاعه أو إنشاء موقع آخر لا تتطلب الوقت والجهد الكثير.
- توفر الأجهزة المستخدمة وقلة التكاليف يسهل من عملية إصلاح وإعادة بناء الشبكات.
- الهجوم في الفضاء السيبراني سريع ولا يمكن معرفة مصدره أو المسؤول عن وقوعه، كونه يحدث من أي مكان في العالم، ما يعطيه الأسبقية عن الدفاع.
- الفضاء السيبراني يتألف من أربع طبقات: البنى التحتية، البني المادية، وطبقتان السيميائية والنحوية، إلا أن السيطرة على إحدى الطبقات لا يعني السيطرة التامة على الفضاء السيبراني.
- لا يعتمد الفضاء السيبراني (cyber pace) كمجال إفتراضي على نظم الكمبيوتر وشبكات الأنترنت ومخزون هائل من البيانات والمعلومات بحيث يتم الإتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من دون تقيد بالحدود الجغرافية.[2]

[1] أنديرا عراجي: **"القوة في الفضاء السيبراني: فصل عصير من التحدي والاستجابة"**. رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية، جامعة لبنان: كلية الحقوق والعلوم السياسية والإدارية، 2016/2015، ص18.

[2] ذويب حسين صابر: **"القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع"**. مداخلة بجمعية المكتبات والمعلومات، الرياض 3-2009/11/4، ص02.

3- مكونات الفضاء السيبراني:

ويتكون الفضاء السيبراني من:[1]

- ✓ الطبيعي أو المادي وهو كل العتاد والأجهزة والكابلات التي ترتبط بالشبكة.
- ✓ المحتوى وهو الشكل الذي تأخذه المعلومات أو البيانات في الفضاء السيبراني.
- ✓ فعالية إدارة عملية الربط بين المعلومات والمستخدمين وبين التفاعل القائم بين المعدات والبرمجيات المستعملة، كون المعلومة أصبحت مهمة للغاية وذات قيمة إقتصادية وعسكرية، فمن يدير المعلومات بكفاءة عالية، يستطيع التحكم والسيطرة في الفضاء السيبراني من خلال عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبر الشبكات.

فالفضاء السيبراني ليس محض افتراضية، وهو يشمل على أجهزة كمبيوتر التي تخزن البيانات بالإضافة إلى الأنظمة والبنية التحتية التي تسمح بالتدقيق وهو يشمل الأنترنت ، الشبكة الداخلية والتقنيات الخلوية وكابلات الالياف الضوئية والإتصالات الفضائية.[2]

ثانيا: الأمن السيبراني:

1- تعريف الأمن السيبراني:

يعرف الأمن السيبراني بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض إتخاذها، أو الإلتزام بها لمواجهة التهديدات، ومنع التعديات أو على الأقل الحد من آثارها.[3]

---

[1] عادل عبد الصادق: "الفضاء الإلكتروني وتهديدات جديدة للأمن القومي". **مجلة الأهرام لكمبيوتر الأنترنت والإتصالات**، مارس 2017، ص3.

[2] Peter w Singer And Allanfriedam, Cybersecurity And Cyberwar, what Everyone Needls to know, USA: University of oxfordpress, 2014.p13.

[3] منى الأشقر جبور: **"السيبرانية هاجس العصر"**. المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 25.

فريتشارد كمرر Richard A . Kemmerer يعرف الأمن السيبراني بأنه :"**عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة**".[1]

بينما عرفه إدوارد أمورسو Edward Amorso على أنه: "**وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها...** إلخ.[2]

وبحسب تعريف الإتحاد الدولي للاتصالات في تقريره حول (إتجاهات الإصلاح في الإتصالات للعام 2010-2011) هو " **مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين**".[3]

وتهدف هذه الحماية إلى ردع المعتدين ومنعهم من تحقيق غاياتهم، مع الحد قدر الإمكان من المخاطر والتهديدات المحتملة، وفق ما يلائم مع المحيط القانوني، التنظيمي، البشري، التقني.

2- أبعاد الأمن السيبراني:

يطال الأمن السيبراني جميع المسائل العسكرية والإقتصادية والإجتماعية، والسياسية والإنسانية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لابد من توضيح أبعاد الأمن السيبراني، التي نوردها كالآتي:[4]

أ- البعد العسكري:

يكمن في الميزة النسبية للقوة السيبرانية التي تعمل على ربط الوحدات العسكرية المختلفة، مما يسمح بتبادل المعلومات وايصال الأوامر العملياتية في أسرع وقت وإصابة الأهداف عن بعد بدقة عالية

---

[1] Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003, p3.

[2] Edward Amoroso, Cyber Security, SiliconPress, 2007, P01.

[3] ITU, Cyber security, Geneva: International Telecommunication Union (ITU) 2008.

[4] عادل عبد الصادق، "القوة الإلكترونية: أسلحة الإنتشار الشامل في عصر الفضاء الإلكتروني". **مجلة السياسة الدولية**، العدد 188، مؤسسة الأهرام، مصر، 2012، ص 32.

إلا أن الشبكات العسكرية تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الإختراق الإلكتروني، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الإتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار صواريخ موجهة، أقمار صناعية.... إلخ)، ويعتبر فيروس ستاكسنت Stuxnet الذي هاجم حواسيب أجهزة الطرد المركزي الإيرانية، بداية لإستعمال القوة السيبرانية لتدمير البنية المادية.[1]

ب- البعد الإقتصادي:

لقد تطور القطاع الإقتصادي بفضل إدخال التكنولوجيات الحديثة عليه والتي تعتمد على الوسائل والتقنيات الرقمية كالدفع الإلكتروني والبطاقات البنكية ومختلف الخدمات الإلكترونية كالبيع والشراء الإلكتروني والتسوق الإلكتروني وتحويل الأموال ...الخ، حيث تعتمد بدرجة كبيرة على الربط بين الشبكات الإلكترونية وسرعة تدفق الأنترنت التي تجعل من جميع العمليات التجارية تتم بسرعة فائقة وبأقل جهد، مما جعل أهمية تحقيق الأمن السيبراني في المجال الاقتصاد يأمرا ضروريا من أجل حماية عمليات تحويل الأموال والحفاظ على أمن معلومات وبيانات الشركات الكبرى والتي هي عرضة للإختراق الإلكتروني أو الإحتيال.[2]

جـ- البعد الإجتماعي:

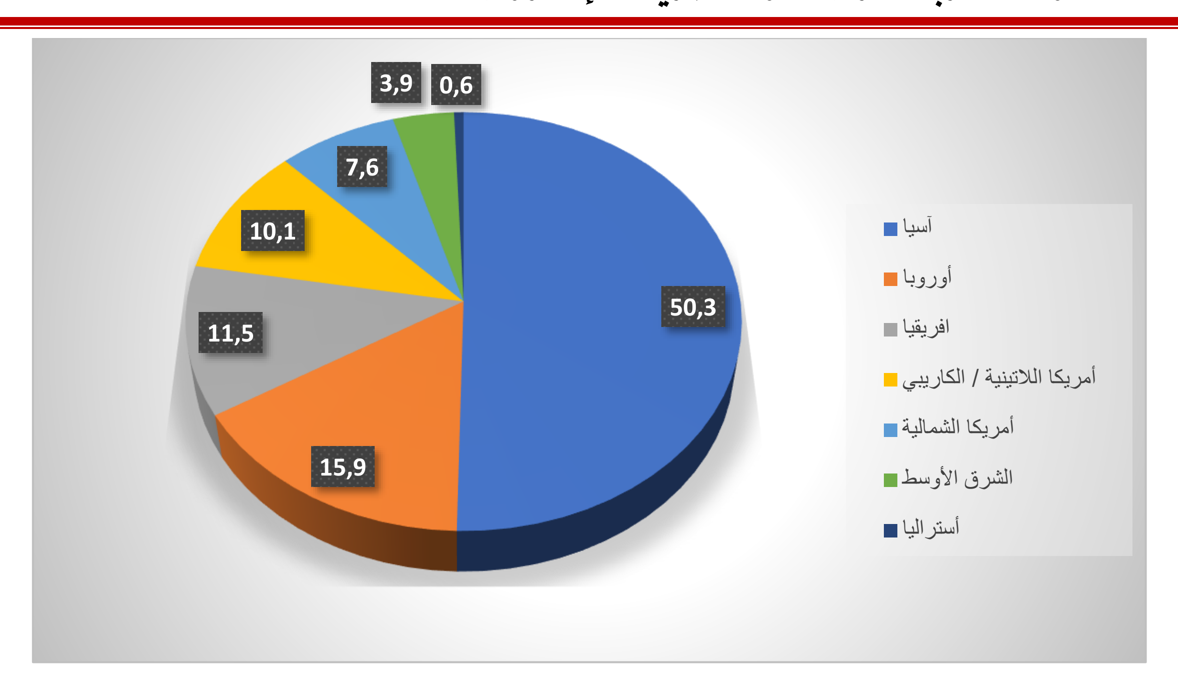
نظرا للعدد الهائل من مستخدمي الانترنيت 4 مليارات شخص في العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل الإجتماعي، ما يجعل منهم أكبر فضاء للتفاعل البشري، يتبادلون الأفكار والمهارات والقيم المجتمعية المختلفة، إلا أنهم معرضون للأخطار بشتى أنواعها كالإختراق الإلكتروني للمعطيات، إنتحال الشخصية، تهديد السلم الإجتماعي للدولة، وعليه لابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الإجتماعي.[3]

---

[1] حمدون تورية: "**الامن السيبراني في البلدان النامية**"، الإتحاد الدولي للاتصالات، 2006، ص15.

[2] منى الأشقر جبور: "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 27-28 أغسطس 2012، ص 16.

[3] الموسوعة السياسية: **الامن السيبراني – cyber security**، على الموقع الإلكتروني: https://political-encyclopedia.org/dictionary/ بتاريخ: 2021/06/01.



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,574,150,134 Internet users in March 3, 2020
Copyright© 2020, Miniwatts Marketing Group

الشكل رقم (01): توزيع مستخدمي الأنترنيت في العالم سنة 2020.

د- البعد السياسي:

يظهر البعد السياسي للأمن السيبراني في حق الدولة بحماية نظامها السياسي ومصالحها الحيوية من أجل تحقيق الازدهار والرفاه لشعوبها، التي أصبحت لاعب أساسي في المنظومة السياسية، وهذا خلال اطلاعها وتأثرها بالكم الهائل من المعلومات المتوفرة بالأنترنت عن الاداء الحكومي، ما جعل السياسيين يستهدفون شريحة معتبرة من الأفراد عبر منصات التواصل الإجتماعي، بهدف الترويج لبرامجهم السياسية، كما أن التدخل الروسي السيبراني في الإنتخابات الأمريكية، أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي.[1]

هـ- البعد القانوني:

إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، كما أن الجريمة السيبرانية تفتقد في

[1] عادل عبد الصادق، "**خطر الحروب السبرانية عبر الفضاء الإلكتروني**"، **مجلة الأهرام لكمبيوتر الأنترنت والإتصالات**، مارس 2017، ص27.

معظم البلدان إلى القوانين الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.[1]

المطلب الثاني: أنواع الجريمة الإلكترونية في الفضاء السيبراني.

تعد الجريمة الإلكترونية من الجرائم المستحدثة التي ظهرت في عصرنا الحديث وكان لها بالغ الأثر على مصالح الأفراد والجماعات والدول، لذلك كان لابد من دراستها ودراسة مرتكبيها من جميع الجوانب التقنية والقانونية والنفسية والإجتماعية...الخ من أجل الوقوف على مختلف أشكالها وأنواعها وبالتالي يسهل مكافحتها من قبل الجهات المختصة بذلك ومن أنواعها نذكر مايلي:

أولا: الجرائم الواقعة على الأشخاص:

إن التطور الذي وصلت إليه البشرية وخاصة في مجال تكنولوجية الإتصال والمعلومات، جعل الأفراد عرضة للعديد من الجرائم، التي يستهدف مرتكبيها سمعة الأشخاص وأموالهم ومعطياتهم الشخصية، مما يسبب لهم أضرار مادية ومعنوية مختلفة.

1-جرائم السب والقذف وتشويه السمعة:

لقد أصبح الفرد عرضة لجميع أنواع القذف والسب التي تسيء إلى شخصه داخل شبكة الأنترنت من خلال ألفاظ وعبارات بذيئة يعاقب عليها القانون، ترسل عبر صفحات الويب، الفيسبوك ما يؤدي بكل من يدخل هذا الموقع لمشاهدتها.[2]

حيث يقوم المجرم بنشر معلومات، قد تكون سرية أو مضللة أو مغلوطة عن الضحية والذي قد يكون فردا، مجتمع، مؤسسة تجارية أو سياسية.[3]

---

[1] اسماعيل قادير،"**ادارة الحروب النفسية في الفضاء الإلكتروني**": الإستراتيجية الامريكية الجديدة في الشرق الأوسط، الندوة الدولية: عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، جامعة الجزائر-03- ،2006، ص 05.

[2] محمد عبيد الكعبي: **"الجرائم الناشئة عن استخدام الغير المشروع لشكة الأنترنت"**. د.ط، دار النهضة العربية، القاهرة، دون سنة، ص 88.

[3] محمد أمين أحمد الشوابكة: "جرائم الحاسوب والأنترنت". د.ط، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004، ص91.

2- جريمة التهديد والمضايقة:

هي توعد الشخص عبر الفايس بوك أو البريد الإلكتروني بإلحاق الضرر به عن طريق الإعتداء عليه أو على ممتلكاته أو أحد أقربائه، ولا يشترط هنا وقوع الفعل على الضحية لتثبت التهمة ضد المجرم لأننا هنا نصبح أمام وصف جزائي آخر مغاير تماما للجريمة الأولى، بل يكفي إيقاع الذعر والقلق والخوف في نفسية الضحية الذي يأمر أو يطلب منه أحيانا القيام بفعل أشياء أو الإمتناع عنها دون رضاه.[1]

3- إنتحال شخصية الفرد:

هي نوع من الجرائم التي تحدث عبر شبكة الأنترنت، والتي يستغل فيها المجرمين هوية الأفراد وبياناتهم ومعطياتهم الشخصية دون علمهم، وتصل إلى درجة التقدم بطلبات لاستخراج البطاقات الإئتمانية إلكترونية، خاصة من الهيئات التي لا تتخذ اجراءات الحماية الامنية الكافية عبر شبكاتها، وهذا ما يستغله المجرم للتصرف في أموال الضحية عن طريق سحب الأموال وتحويلها أو شراء منتجات إستهلاكية.[2]

حيث تشير هيئات شركات البطاقات الإئتمانية من طرفها إلى أن نسبة إنتحال الشخصية ضعيفة جدا مقارنة بمئات المليارات من الدولارات التي تنفق عبر البطاقات الإئتمانية سنويا.

4- صناعة ونشر الإباحة:

وجود مواقع على شبكة الأنترنيت تحرض على ممارسة الجنس للكبار والقصّر، وذلك بنشر صور جنسية للتحريض على ممارسة المحرمات، والجرائم المخلة بالحياء عن طريق صور، أفلام، رسائل...إلخ

---

[1] منال مباركي: المرجع السابق، ص72.

[2] رشيدة فاريس، نورة قأوش: **"تأثير مواقع التواصل الإجتماعي في إنتشار الجريمة الإلكترونية في وسط المراهقين".** دراسة ميدانية بثانوية كريم بلقاسم بولاية البويرة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والإتصال تخصص اتصال ومجتمع، جامعة أكلي محند والحاج، كلية العلوم الإنسانية والإجتماعية، قسم العلوم الإنسانية، البويرة، 2018/2017، ص 68.

وذلك ما يعتبر جريمة يعاقب عليها القانون[1]، كما أن شبكة الأنترنت توجد بها ألاف المواقع التي تروج وتسوق للدعارة دون أية سيطرة من قبل القوانين الوطنية أو الدولية، توفر للمجرمين خيارا جديدا للغاية لتسهيل الدعارة.[2]

ثانيا: الجرائم الواقعة على الأموال والأنظمة:

بفضل ارتباط العديد من المؤسسات التجارية والمالية والإقتصادية بشبكة الأنترنت، فإن جل خدماتها إلكترونية لم تعد تتطلب تنقل الزبون وقيامه بالمعاملات التقليدية كدفع للأموال وتحويلها أو سحبها، ما جعلها محل أطماع العديد من المجرمين للإختراق أنظمتها الإلكترونية والاستيلاء على أموال مستعمليها.

1- السرقة عبر الأنترنت:

هي تلك الجرائم التي يتم عبرها السيطرة على معلومات فكرية مملوكة للغير أو الاستيلاء على ديسكات أو أقراص مكتنزة، تتضمن محتويات أو مواد أنتجها الآخرون، وكل هذه الأفعال الإجرامية تحدث بواسطة تكنولوجيا المعلومات[3]، إلا أنها غالبا لا تفعل غرض إجرامي بل قد يلجا إليها على سبيل المثال لتحرير بطاقات مخصصة لأعمال الخير أو نسخ ألعاب الفيديو للإستعمال الشخصي، و تتم سرقة منفعة الحاسب الآلي بالاستخدام الغير المشروع للأنظمة المعلوماتية (Data Processing Systems DP) أو سرقة الخدمة المعلوماتية، فهي تقتصر على وقت وجهد الآلة دون نية إختلاس البيانات والمعلومات وهي تشبه فعل إستعمال أشياء الغير بدون وجه حق.[4]

---

[1] سورية ديش: "أنواع الجرائم الإلكترونية وإجراءات مكافحتها". **مجلة العلوم السياسية والقانون**، العدد 01، الجزائر، 2017، على الموقع الإلكتروني:

https://democraticac.de/?p=43845 بتاريخ: 2021/06/02 على الساعة: 22:30.

[2] كريستاس كولمان: "**عن جرائم الانترنيت طبعتها وخصائصها**". الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 يونيو 2007، ص: 40.

[3] عبد الحكيم رشيد توبة: **"جرائم تكنولوجيا المعلومات"**. ط1، دار المستقبل للنشر والتوزيع، الأردن، 2008، ص 189.

[4] منال مباركي: مرجع سابق، ص73.

2- الإحتيال الإلكتروني:

هي جريمة يقوم المجرم فيها على إستغلال الحاسوب للحصول على مبالغ نقدية غير مشروعة له أو لغيره، وذلك نتيجة عملية معالجة المعلومات من خلال صيغة خاطئة للبرنامج أو عن طريق إستعمال غير مرخص للمعلومات،[1] ويتم ذلك بطريقة إحتيالية عن طريق ايهام المجني عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح، فيسلم المال للجاني عن طريق الأنترنت أو من خلال تصرف الجاني في المال، رغم علمه بأن ليس له صفة التصرف فيه.[2]

3- التحويل الإلكتروني للأموال:

هي العملية التي تتم بواسطة الحاسب الآلي عبر شبكة الأنترنت، من أجل تلبية الاحتياجات المختلفة للعملاء والبنوك والمتاجر والعاملين، وهذا وفق نظام معلوماتي متكامل من أجل تحصيل قيمة السلع والخدمات أو تحويل الأموال أو دفع المرتبات، حيث يسيطر المجرمين على هذا النظام بطريقة غير مشروعة ويقومون بتحويل الأموال إلى غير وجهتها الحقيقية.[3]

4- الإرهاب الإلكتروني:

يمارس العنف المعلوماتي أو الإرهاب الإلكتروني عبر القوى اللينة التي تختلف جوهريا عن القوى التقليدية الصلبة، فهي تعمل بالجذب لا بالضغط وبالترغيب والترهيب،[4]حيث تلجأ إلى الاعلام والدعاية من خلال بث فيديوهات بالمواقع إلكترونية، تمجد الإرهاب أو تدعوا إلى تجنيد الأفراد في صفوفه بغرض تنفيذ عمليات إجرامية.

5- الإختراق الإلكتروني:

عملية الإختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الأنترنت وهي عملية يمكن حدوثها من أي بلد في العالم، دون الحاجة إلى التواجد الجسدي للمجرم في

---

[1] نفسه، ص 74.

[2] ندوة التنمية ومجتمع المعلوماتية: **"الجريمة المعلوماتية"**. الجمعية السورية للمعلوماتية، حلب، 2000، ص5.

[3] نائلة عادل محمد فريد قورة: **"جرائم الحاسب الآلي الإقتصادية"**. دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية، 2005، ص 496.

[4]عبد الحكيم رشيد توبة، مرجع سابق، ص 174.

البلد الذي يتعرض للإختراق، كما لا يتم بضرورة إكتشاف هذه الإختراقات بسبب التعقيد الذي تتصف به نظم تشغيل الحاسبة الإلكترونية.[1]

[1]عزيزة رباحي: "**الأسرار المعلوماتية وحمايتها الجزائية**". أطروحة مقدمة لنيل درجة الدكتوراه في القانون، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، سنة 2017–2018، ص112.

المبحث الثالث: أشكال التعاون الدولي لمواجهة الجريمة الإلكترونية:

إن التطور السريع لتقنيات تكنولوجيا المعلومات، أدى إلى عدم اعتراف المجرم الإلكتروني بالحدود الجغرافية للدول، مما جعل التنسيق الدولي والإقليمي ضرورة ملحة، من أجل التكيف مع المستجدات ووضع الآليات المناسبة قصد التصدي للجرائم الإلكترونية، وهذا لا يكون إلا من خلال التعاون مع الأجهزة الأمنية والقضائية الدولية التي يخول لها القانون متابعة المجرمين وتوقيفهم أينما كانوا من أجل تقديمهم للعدالة ومعاقبتهم، حسب ما ينص عليه تشريع كل دولة.

المطلب الأول: المجهود الدولي والإقليمي في مكافحة الجريمة الإلكترونية.

لقد بذلت الكثير من الدول مجتمعة جهودا معتبرة، عبر الهيئات والمنظمات الدولية والإقليمية المنخرطة بها، من أجل بلورة عمل دولي مشترك لمواجهة الجرائم المستحدثة، والتي يمكن أن نذكر جملة من هذه المجهودات المتمثلة فيما يلي:

أولا: على المستوى الدولي:

1- منظمة الأمم المتحدة:

تبذل الأمم المتحدة جهودا معتبرة في مجال محاربة الجريمة الإلكترونية وأساليب التصدي لها مؤكدة دائما على ضرورة العمل المشترك بين أعضاء المنظمة وتكاتف الجهود للحد من إنتشارها وتعاظم آثارها، وذلك من خلال متابعتها وإشرافها على عقد المؤتمرات الدولية وعمل الوكالات والمنظمات النشطة تحت لوائها.[1] حيث عملت في مؤتمرها الثامن المنعقد في هافانا عام 1990 حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجراء الدولي لمواجهة جرائم الأنترنت يتطلب من كل دولة عضو تحديث القوانين وأغراضها الجنائية، قبول الأدلة على نحو ملائم وإدخال تعديلات تشريعية، اتخاذ تدابير الأمن والوقاية مع الحفاظ على خصوصية الأفراد وحقوق الانسان، رفع الوعي لدى الجماهير والقضاة والأجهزة المكلفة بمكافحة هذا النوع من الجرائم،

---

[1] نعيم سعيداني: "**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**"، مذكرة مقدمة لنيل شهادة الماجستير في القانون، جامعة الحاج لخضر– باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2013/2012، ص83.

التعاون مع مختلف المنظمات المهتمة بهذا الشأن، ووضع وتدريس مناهج تراعي آداب استخدام الحاسوب، حماية مصالح الدولة وحقوق ضحايا جرائم الأنترنت.[1]

لقد أدى تزايد الجرائم المرتكبة عبر الأنترنت بمنظمة الأمم المتحدة إلى عقد الإتفاقية الخاصة بمكافحة إساءة إستعمال التكنولوجيا لأغراض إجرامية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول بخصوص هذا الشأن، بالإضافة إلى الدور الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية.[2]

كذلك عمدت اللجنة الإقتصادية والإجتماعية لغربي آسيا التابعة للمجلس الإقتصادي والإجتماعي، وذلك تحت غطاء منظمة الأمم المتحدة على عقد ورشة عمل حول التشريعات السيبرانية وتطبيقها في منطقة الإسكوا عام 2008.[3]

كما عقدت منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12_19 أفريل 2010، حيث احتل موضوع الجرائم الإلكترونية موقعا بارزا في جدول أعمال المؤتمر، حيث ناقشت المخاطر وتكنولوجيا الحاسوب المستخدمة ودور الأجهزة المكلفة بمحاربتها وذلك تأكيدا على خطورتها والتحديات التي تطرحها.[4]

ودعت لجنة منع الجريمة والعدالة الجنائية إلى عقد إجتماع لفريق من خبراء حكومي دولي مفتوح العضوية من أجل دراسة شاملة حول الجريمة السيبرانية من خلال التطرق إلى أساليب مكافحتها وأسباب

---

[1] نعيم سعيداني: المرجع السابق، ص 94.

[2] إتفاقية مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (55/63)، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة 81، ديسمبر 2000.

[3] اللجنة الإقتصادية والإجتماعية لغربي آسيا (الإسكوا)، ورشة عمل حول التشريعات السيبرانية تطبيقها في منطقة الإسكوا، ببيروت 15_16 ديسمبر 2008، المجلس الإقتصادي والإجتماعي التابع للأمم المتحدة، رقم E/ESCWA/ICTD/2009/1

[4] مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12_19 أفريل 2010، رقم 9/ A /conf.213

إنتشارها ودوافع إرتكابها ودراسة مدى تطابق التشريعات مع الإجرام السيبراني، كذلك إجراءات التحقيق التعاون الدولي، المساعدة التقنية الدولية ودور القطاع الخاص في الحد من الجريمة.[1]

بالإضافة إلى العديد من المؤتمرات المتعلقة بإتفاقية مكافحة الجريمة المنظمة عبر الوطنية المنعقد بفيينا في أكتوبر 2010، حدد المؤتمر فهرس الأمثلة المتعلقة بالتعاون الدولي مثل تسليم المجرمين وتبادل المساعدة القانونية...إلخ، أما لجنة حقوق الطفل التابعة لمنظمة الأمم المتحدة فقد عقدت إتفاقية خاصة بحقوق الطفل من أجل النظر في الجرائم التي ترتكب في حق الطفولة منها إستغلالهم في المواد الإباحية عبر الأنترنت.[2]

2- منظمة التعاون الإقتصادي والتنمية:

رغم أن هذه المنظمة تهدف إلى تحقيق أعلى مستويات النمو الإقتصادي وتناغم التطور الإقتصادي مع التنمية الإجتماعية، إلا أنها منذ عام 1978 أظهرت الاهتمام بالجرائم المرتكبة عبر الأنترنت، وذلك بوضعه المجموعة من الأدلة والقواعد الإرشادية التي تتصل بتقنية المعلومات، حيثيعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات، من الأدلة الرئيسية التي تم الاعتماد عليها في عام 1980 من قبل مجلس المنظمة، مع توصية الأعضاء بالالتزام بها.[3] وأصدرت عام 1983 تقريرا بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، استعرض السياسة الجنائية القائمة ومقترحات الدول الأعضاء، وتضمن أمثلة عن أفعال سوء استخدام الحاسوب مثل: الاستخدام أو الدخول إلى نظام ومصادر الحاسب دون تصريح مسبق، الإفشاء غير المصرح به للمعلومات المعالجة أليا والنسخ إتلاف أو تخريب ما يحتويه من بيانات وبرامج، أين تم تجريم هذه الأفعال ووضع التشريع الذي يتناسب وقوانين الدولة.[4]

---

[1] إجتماع فريق الخبراء المعني بالجريمة السيبرانية، "**مشروع المواضيع المطروحة لنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية وتدابير التصدي لها**". فيينا 17_21 جانفي 2011، رقم UNODC /ccpcj /cg 4/2011/2.

[2] إتفاقية حقوق الطفل، النظر في التقارير المقدمة من الدول بموجب الفقرة امن المادة 12 من البروتوكول الاختياري لإتفاقية حقوق الطفل المتعلق ببيع وبغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة السابعة والخمسون، 30 ماي 17 جويلية 2011، الأمم المتحدة، رقم:CRC/c/opsc/egy/co/1

[3] غازي عبد الرحمان هيان الرشيد: "**الحماية القانونية من جرائم المعلوماتية (الحاسب والأنترنت)**". أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص179.

[4] نفسه، ص ص 179، 180.

كما وضعت المنظمة عام 1992 من خلال الملتقيات وورشات العمل التي نظمتها مع القطاعات المهتمة بهذا الشأن، توصيات إرشادية خاصة بأمن أنظمة المعلومات، مع التوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء الأفعال التالية:

1) التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
2) التجسس المعلوماتي ويندرج تحته الحصول أو الإقتناء أو الإستعمال غير المشروع للمعطيات.
3) التخريب المعلوماتي ويندرج تحته الإستخدام غير المشروع أو سرقة وقت الحاسب.
4) قرصنة البرامج.
5) الدخول غير المشروع على البيانات أو نقلها.
6) اعتراض استخدام المعطيات أو نقلها.[1]

3- المنظمة العالمية للملكية الفكرية:

تعد هذه المنظمة إحدى الوكالات التابعة للأمم المتحدة، وقد اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم، بهدف تشجيع النشاط الابتكاري، وتطوير إدارة الإتحادات المنشأة في مجالات حماية الملكية الصناعية، وحماية المصنفات الأدبية والفنية.[2] حيث تهتم هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، إلا أن تشريعات براءات الاختراع عجزت في توفير هذه الحماية، أين لجأت إلى الاتفاقيات العالمية وخاصة مثل "التربس" و"برن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها وخاصة تشريعات حق المؤلف[3]، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمرتكبة في إطار تجاري، وبالطبع تعتبر الأنترنت من الأماكن الخصبة لهذا النوع من التصرفات[4] والتي استطاعت توفير الحماية القانونية للبرامج وقواعد البيانات المعلوماتية.

---

[1] يوسف صغير: "**الجريمة المرتكبة عبر الأنترنت**". مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص94.

[2] عبد الرحمن جميل محمود حسين: "**الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة**". رسالة مقدمة لنيل شهادة الماجستير في القانون الخاص، جامعة النجاح الوطنية، كلية الدراسات العليا سنة 2008، ص ص 86، 87.

[3] غازي عبد الرحمن هيان الرشيد، مرجع سابق، ص 181.

[4] جون فرنسوا هنروت: "**أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي**". أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19-20 يونيو 2007، ص98.

ثانيا: على المستوى الاقليمي:

1- المجلس الأوروبي:

صدرت دراسة له عام 1989 تناولت توصيات تفعيل دور القانون لمواجهة الأفعال الغير مشروعة عبر الحاسوب، وفي عام 1995 قام المجلس الأوروبي بدراسة أخرى تضمنت الإجراءات الجنائية في مجال الجرائم المعلوماتية، وعلى ضوء التوصيات السابقة، قام عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد إتفاقية في هذا الإطار.[1]

وقد تم وضع إتفاقية من قبل مجلس أوربا بالتعاون مع العديد من الدول على غرار كندا، اليابان جنوب إفريقيا ،الولايات المتحدة الأمريكية وقع عليها في بودابستعام 2001 ودخلت حيز التنفيذ عام 2004 وهي لا تقتصر على أي اقليم معين بل تعنى جميع دول التي تبدي رغبة في ذلك، حتى أن هذه الإتفاقية أصبحت نموذجا يحتذى به للكثير من الدول في صياغة تشريعاتها بشأن جرائم الأنترنت مثل الأرجنتين، والبرازيل وكولومبيا، والهند، واندونيسيا وغيرها، كما أن للمجلس الأوروبي العديد من المساهمات، نذكر منها على سبيل المثال إتفاقية 28 جانفيعام 1981 المتعلقة حماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات ذات الصبغة الشخصية، إلا أن إتفاقية بودابست تبقى الحيز الأمثل لمواجهة مختلف الجرائم عبر الأنترنت.[2]

2- الدول العربية:

إن كثرت المعلومات المتداولة في الدول العربية، أدى إلى ظهور العديد من الأفعال الإجرامية مما فرض على هذه الدول أن تعمل على ايجاد الحيز التشريعي والإجرائي الناجع لمواجهة هذا النوع من الجرائم المستجدة.[3]، وهذا ما يوضحهقرار إصدار قانون جزائي موحد ، كقانون عربي نموذجي صادر عن مجلس وزراء العدل العرب، وفيه الباب السابع المتعلق بالجرائم ضد الأشخاص، قد إحتوى على فصل خاص بالإعتداء على حقوق الأشخاص المرتبطة أساسا بالمعالجات المعلوماتية، وذلك في المواد 461-

---

[1] نعيم سعيداني، مرجع سابق، ص 85.

[2] يوسف صغير، مرجع سابق، ص ص، 101.100

[3] عباس أبو شامة عبد المحمود: "**التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية**" الندوة العلمية، الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس أيام 28-30 جوان 1999، ص50.

464 التي أشارت على وجوب حماية الحياة الخاصة، وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها وعقوبة إرتكاب مثل هكذا جرائم.[1]

كما تم إبرام الإتفاقية العربية لحماية حقوق المؤلف في مجال الملكية الفكرية، والتي تنص على توفير الحماية القانونية للبرامج المعلوماتية (برامج الحاسب الآلي)، مع الحث والتشجيع المتواصل للدول الأعضاء على تحديث وتطوير تشريعاتها الجزائية من أجل مكافحة الجرائم المرتكبة عبر الأنترنت.[2]

غير أن الملاحظ في هذه المحاولات على المستوى العربي، أنها تعمل في مجملها على ملأ الفراغ القانوني والتشريعي المرتبط بموضوع جرائم الأنترنت، وذلك من خلال:[3]

– وضع أطر عامة حول ضوابط استخدام وأمن الأنترنت وذلك بتحديد النشاطات الإجرامية التي توظف بالشبكات المعلوماتية.

– إصدار تعليمات متعلقة بأمن المنشئات الحاسوبية والأجهزة والبرامج المعلوماتية.

– تحديد القواعد العامة المنظمة للارتباط المنشئات الحكومية بالشبكة العالمية.

3- مجموعة الدول الثمانية:

تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات البحثية والتطبيقية في مختلف الموضوعات التي تهم المنظمة، وهي ليست إطارا تشريعيا للدول الأعضاء، ولكنها تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك، لبلورة خطط عملية كحصيلة لتوجيهات قادة هذه الدول ومكافحة كل ما من شأنه التأثير أو تهديد أمن وإستقرار الدول الأعضاء.[4]

اعتمدت مجموعة الدول الثمانية من خلال إجتماع عقده وزراء عدل هذه الدول بواشنطن، يومي التاسع والعاشر من ديسمبر 1997، المبادئ التي تشكل الأساس لشبكة نقاط اتصال وطنية، كما تم

---

[1] تركي بن عبد الرحمن المويشر: "**بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليتها**". أطروحة دكتورة الفلسفة الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، كلية الدراسات العليا، سنة 2009 ص 175.

[2] محمود أحمد عبابنة: "**جرائم الحاسوب وأبعادها الدولية**". دط، دار الثقافة للشر والتوزيع، الأردن، سنة 2005، ص 181.

[3] فايز بن عبد الله الشهري: "التحديات الأمنية المصاحبة لوسائل الإتصال الجديدة (دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الأنترنت)". **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 20، العدد 49، 2005، ص 153.

[4] غازي عبد الرحمن هيان الرشيد، مرجع سابق، ص 184.

وضع خطة عمل لإنشاء شبكة متابعة، والتي تعمل على اعداد التقارير عن مدى التزام كل دولة في الشبكة، وقد أنشئت على غرار نموذج الإنتربول في الفترة ما بين 1998 و2000 وتعمل على مواصلة تكثيف الجهود من أجل انضمام ومشاركة أكبر عدد من الدولة.[1]

كما تناولت في المؤتمر الذي عقدته في باريس في عام 2000، موضوع الجريمة السيبرانية وذلك بحثها على منع الملاذات الرقمية التي تعمل خارج القانون، أخذت إتفاقية مجلس أوربا بشأن الجريمة السيبرانية أساسا لمحاولاتها الرامية إلى إيجاد حلول دولية، وفي عام 2001 قامت بعقد ورشة عمل بطوكيو ناقشت من خلالها الادوات الإجرائية لمحاربة الجريمة السيبرانية، ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو أن حفظ البيانات يعد حلا بديلا.[2]

ما يلاحظ أنه بالرغم من جهود الهيئات والمنظمات الدولية والإقليمية وما صدر عنها من توصيات وإتفاقيات بخصوص مكافحة الجريمة الإلكترونية، إلا أنها لم تخرج في مضمونها عن تعداد ووصف لهذه الجرائم المستحدثة، مما يتطلب من جميع الدول المشاركة في هذا المسعى المزيد من بذل الجهود والتنسيق فيما بينها، من أجل ايجاد آليات عملية، للحد من الجرائم المرتكبة في الفضاء الافتراضي.

المطلب الثاني: التعاون الأمني والقضائي الدولي لمكافحة الجريمة الإلكترونية.

أولا: على المستوى الأمني

لقد أصبحت الدول بأمس الحاجة إلى وجود كيان دولي، تتشارك من خلاله وضع الآليات وتنفيذ الإستراتيجيات الدولية بالتنسيق والتعاون مع مختلف الأجهزة الشرطية، خاصة فيما يتعلق بسرعة تبادل المعلومات المتعلقة بالمجرمين المبحوث عنهم والجرائم المستحدثة والمنظمة العابرة للحدود وغيرها.

1- جهود المنظمة الدولية للشرطة الجنائية "الإنتربول":

لقد عرف التعاون الدولي الشرطي عام 1904 منذ إبرام الإتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 1904/05/18، والتي جاء في مادتها الأولى "تتعهد كل الحكومات المتعاقدة بإنشاء أو

---

[1] يوسف صغير، مرجع سابق، ص 102.

[2] نفسه، ص 102.

تعين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة".

بعد ذلك شهد هذا التعاون العديد من المؤتمرات الدولية نذكر منها[1]: أول مؤتمر بموناكو شاركت فيه أربعة عشر دولة، إنعقد من 14-18 أفريل 1914 بفرنسا، وقد ضم رجال الشرطة والقضاء، ناقشوا فيه وضع أولى لبينات التعاون الدولي في المسائل الشرطية، في مقدمتها إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، إلا أن هذا المؤتمر لم يحقق أهدافه نظرا لظروف التي عرفها العالم أثناء الحرب العالمية الأولى، بعدها عقد مؤتمر دولي في الفترة 03-07 سبتمبر 1946 يعد الثاني على المستوى الدولي للشرطة الجنائية ، ضم مندوبي تسعة عشر دولة، كان من أهم قراراته انشأ اللجنة الدولية للشرطة الجنائية مقرها فيينا، وظيفتها الأساسية التنسيق بين أجهزة الشرطة للتعاون في مكافحة الجرائم، وفي بروكسل ببلجيكا في الفترة 06-09 جوان 1946 بدعوة من المفتش العام للشرطة البلجيكية عقد مؤتمر دولي آخر بغرض تفعيل مبادئ التعاون الأمني وتطبيق الالتزامات السابقة، خاصة فيما يخص عمل اللجنة الدولية للشرطة الجنائية[2]، نقل مقرها إلى باريس بفرنسا وتغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية والتي تضم في عضويتها 182 عضوا.[3]

تهدف هذه المنظمة إلى التعاون بين أجهزة الشرطة في الدول الأعضاء، مكافحة جميع أنواع الجرائم جمع المعلومات والبيانات حول الجريمة ومرتكبيها، وهذا بالاعتماد على المكاتب المركزية الوطنية للشرطة الدولية الموجودة في جميع الدول المنخرطة بالمنظمة[4]، وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة جميع أجهزة الشرطة في الدول الأعضاء[5]، مع تزويدها بالمعلومات المتوفرة لديها على اقليم اختصاصها وخاصة بالنسبة للجرائم المنتشرة في عدة دول ومنها جرائم الأنترنت، مثال على ذلك تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بخصوص قيام طالب جامعي بإرسال

---

[1] علاء الدين شحاتة: "**التعاون الدولي لمكافحة الجريمة**"، د.ط، إيتراك للنشر والتوزيع، القاهرة، 2000، ص ص174، 176.

[2] تم وضع ميثاق هذه المنظمة في الفترة ما بين 7-13 جوان 1956 وأعتبر نافذا من 13 جوان 1956.

[3] Malom Aderson policing the world Interpol the politics of international police co-operation clarendon Press .oxford.1989 p185-186.

[4] جميل عبد الباقي الصغير: "**الجوانب الإجرائية للجرائم المتعلقة بالأنترنت**". ط1، دار النهضة العربية، القاهرة 1998م ص 71.

[5] محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الإلكترونية". **المجلة الأكاديمية للبحث القانوني**، المجلد 14، العدد 02، المملكة العربية السعودية، 2016/11/27، ص53.

صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الأنترنت، أين تم توقيفه من قبل القضاء اللبناني باعتباره مرتكب لجريمة يعاقب عليها القانون.[1]

وعلى غرار هذه المنظمة **أنشأ المجلس الأوربي في لكسمبورج عام 1991 شرطة أوربية** تعمل على التنسيق والربط بين أجهزة الشرطة الوطنية في الدول الاعضاء، من أجل ملاحقة مرتكبي الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالأنترنت.[2]

أما على المستوى العربي نجد أن **مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية** بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة من أجل دعم وتطوير أجهزة الشرطة في الدول العربية.[1]

2- تبادل المعاونة لمواجهة الأخطار والأزمات:

تبادل المهارات والخبرات من صور التعاون الدولي في المجال الأمني بين الدول، وهذا راجع إلى التفاوت الموجود بين هذه الأجهزة، والتي منها من تمتلك المستوى الفني والتقني والتكنولوجي الذي يمكنها من مواجهة الجرائم الإلكترونية، بينما تفتقد أجهزة العدالة الجنائية الأخرى هذا المستوى، ما جعل من محاربة الجرائم المتعلقة بالأنترنت أمر في غاية الصعوبة، من هنا كان لابد من التعاون بين الدول.[3]

3- القيام ببعض العمليات الشرطية والأمنية المشتركة:

هناك بعض الجرائم التي تتطلب القيام بعمليات مشتركة بين الشرطة والأجهزة الامنية المختلفة وخاصة تلك المتعلقة بالجرائم الإلكترونية العابرة للحدود، أين تحتاج تعقب مجرمي المعلوماتية وشبكة الأنترنت وجمع المعلومات والقيام بعملية تفتيش إلكتروني للمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الإتصال بحثا عن الأدلة الرقمية التي من شأنها ادانة المجرمين وتوقيفهم؛ كلها مسائل تحتاج إلى التنسيق الشرطي والأمني وتبادل للاستشارات والخبرات من أجل فعالية أنجع للحد من هذه الجرائم.[4]

---

[1] محمد أحمد سليمان عيسى: المرجع نفسه، ص54.

[2] جميل عبد الباقي الصغير، مرجع سابق، ص 79.

[3] محمد أحمد سليمان عيسى، مرجع سابق، ص 54.

[4] المرجع نفسه، ص 54.

ثانيا: على المستوى القضائي

يعتبر التعاون القضائي الدولي من أهم أشكال التعاون بين الدول، وأكثرها فعالية في مواجهة الجرائم الإلكترونية، التي تقتضي مساعدة من سلطات البلد الذي يعد منشأ للجريمة أو من سلطات البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف أو حيث قد توجد أدلة الجريمة فقد يكون مرتكب الجريمة يحمل جنسية دولة ما، إلا أنه يستعمل في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة، أين يصبح مبدأ السيادة ومشاكل الحدود والتشريعات القضائية الوطنية عقبة أمام إكتشاف هذه الجرائم ومتابعة مرتكبيها وتوقيفهم، وهذا ما يؤكد على أهمية المساعدة القضائية المتبادلة بين الدول.[1]

1- المساعدة القضائية الدولية:

هي من مظاهر التعاون الدولي التي تستعين بها الجهات القضائية في دولة ما من أجل ملاحقة مجرمين فارين في دول أخرى وعادة ما تتم عن طريق الاتفاقيات بين دولتين أو أكثر، حيث يتم النظر في الطلب إن كان مبررا وهناك ضمانات لإخضاع المجرمين لمحاكمة عادلة.[2]

2- تبادل المعلومات:

يقصد بها أن تقوم سلطة قضائية في دولة أجنبية ما، بصدد معالجة قضية جنائية تخص رعاياها أو رعايا بلد آخر ثبت تورطهم فيها، طلب تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية...إلخ، والتي تساعد على إثبات تورطهم وقد يشمل أيضا تتبادل السوابق القضائية للجناة.[3]

3- نقل الإجراءات:

تعني قيام دولة بناء على إتفاقية أو معاهدة باتخاذ إجراءات جنائية في حق مجرمين، يكونون قد إرتكبوا جرائم في دولة أخرى وهذه الإجراءات تتم لمصلحة هذه الدولة، شريطة أن تكون الأفعال المقترفة مجرمة في كلتا البلدين، وأن تكون الإجراءات المطلوب إتخاذها تؤدي دورا مهما في الوصول إلى

---

[1] نعيم سعيداني، مرجع سابق، ص89.

[2] عباسي محمد الحبيب، "**الجريمة المنظمة العابرة للحدود**". أطروحة مقدمة لنيل شهادة الدكتوراه تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، الجزائر، 2017/2016، ص 590.

[3] محمد أحمد سليمان عيسى، مرجع سابق، ص55.

الحقيقة[1]، كما أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية.[2]

4- الإنابة القضائية الدولية:

هي إجراء من إجراءات الدعوى العمومية، تطلب دولة بموجبه من دولة أخرى ضرورة الفصل في مسألة جنائية معروضة على السلطة القضائية للدولة الطالبة ويتعذر عليها القيام به بنفسها.[3]

ويهدف هذا الاجراء إلى تسهيل عمل السلطات القضائية، كما يضمن القيام بالتحقيقات اللازمة وتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تقف حائلا دون ممارسة الدول الاجنبية للأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيرها.

ونظرا لأن مثل هذه الإجراءات قد تتخذ وقتا طويلا فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت اختصار الإجراءات عن طريق الإتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الإتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال[4]، ونفس الشيء نجده في البند الثاني من المادة 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999م والمادة 15 من إتفاقية الرياض العربية للتعاون القضائي 1983، والمادة 53 من إتفاقية شينغن 1990 والخاصة باستخدام الإتصالات المباشرة بين السلطات القضائية في الدول الأطراف، والفقرة 13 من المادة 46 من إتفاقية الأمم المتحدة لمكافحة الفساد.[5]

5- تسليم المجرمين:

بما أنه لا يمكن لأي دولة أن تتجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين خارجها، كان لابد من إيجاد آلية للتعاون مع الدول التي ينبغي اتخاذ الإجراءات القضائية فوق

---

[1] محمد أحمد سليمان عيسى، مرجع سابق، ص55.

[2] نعيم سعيداني، مرجع سابق، ص91.

[3] عبد الرؤوف مهدي: "**شرح القواعد العامة للإجراءات الجنائية**". دط، دار النهضة العربية، الإسكندرية، 1996، ص 102.

[4] جميل عبد الباقي الصغير: "**الجوانب الإجرائية المتعلقة بالأنترنت**". ط2، دار النهضة العربية، الاسكندرية، 2002، ص83.

[5] محمد أحمد سليمان عيسى، مرجع سابق، ص56.

أقاليمها وهذا الإجراء يقوم أساسا على أن أي دولة يتواجد على ترابها المتهم بإرتكاب جريمة إلكترونية، وجب عليها أن تقوم بمحاكمته إن كانت تشريعاتها تسمح بذلك، وإلا تقوم بتسليمه للجهة الطالبة من أجل نفس الغرض، وهذا حتى تتحقق العدالة وينال الجناة عقابهم، لذلك حرصت معظم الدول على إبرام الاتفاقيات والمعاهدات وسن التشريعات الخاصة بتسليم المجرمين.[1]

[1] نعيم سعيداني، مرجع سابق، ص91.

خلاصة الفصل الأول:

إن الجريمة الإلكترونية من الجرائم المستحدثة ذات طبيعة خاصة، يرتكبها مجرمين يتميزون بالمهارة والذكاء ومتحكمين بتكنولوجيا المعلوماتية، ما جعلها صعبة الإكتشاف وتحتاج لقوانين وطنية ودولية تعنى بجميع جوانبها، لذلك لا يمكن للدول أن تواجهها بمفردها، كونها عابرة للحدود وقد تسبب أضرار بالغة بالأفراد والمؤسسات، وهذا جعلها شكل جديد من أشكال التهديدات الأمنية السيبرانية وعلى أساس ذلك جاء التعاون الدولي بآليات تشريعية وأمنية وسياسية عبر مختلف المنظمات والهيئات الدولية على غرار منظمة الأمم المتحدة ومنظمة الإنتربول...الخ، قصد وضع إستراتيجية دولية لمحاربة الجريمة الإلكترونية ومحاسبة مرتكبيها وفقا للقوانين الصادرة في هذا الخصوص.

الفصل الثاني:

السياسة الأمنية الجزائرية في محاربة الجريمة الإلكترونية

تمهيد:

إدراكا من الدولة الجزائرية لحجم التهديدات التي أصبحت تحملها الثورة التكنولوجية للإتصال والمعلوماتية، والرغبة الجادة منها في مواجهة الجريمة الإلكترونية، عملت على وضع الآليات التشريعية والمؤسساتية الضرورية وإبرام الإتفاقيات الدولية...إلخ، كما قامت بإقحام مختلف الأجهزة الأمنية بفرقها العملياتية ومراكزها ومعاهدها المتخصصة، ما ساهم في كشف العديد من الجرائم وملاحقة مرتكبيها وتسليمهم للعدالة.

ومن أجل توضيح ذلك قمنا بتقسيم الفصل الثاني إلى ثلاثة مباحث التالية:

المبحث الأول: واقع الجريمة الإلكترونية في الجزائر.

المبحث الثاني: آليات مكافحة الجريمة الإلكترونية في الجزائر.

المبحث الثالث: التحديات والآفاق في مكافحة الجريمة الإلكترونية بالجزائر.

المبحث الأول: واقع الجريمة الإلكترونية في الجزائر.

لقد عرفت الجزائر كغيرها من دول العالم تطورا في مجال الإعلام الآلي وتكنولوجيا الإتصالات والمعلومات، وعلى الرغم من حداثة التوجه الجزائري نحو الحوكمة الإلكترونية، إلا أن عدد الجرائم الإلكترونية المرتكبة يوحي بحجم الأخطار التي تتربص بها، وهو ما يجعلها أمام تحديات وعوائق جديدة تتمثل في تحقيق الأمن الإلكتروني حاليا ومستقبلا.

المطلب الأول: الإحصائيات الوطنية للجرائم الإلكترونية.

يرجع إرتفاع معدل الجريمة الإلكترونية في الجزائر إلى زيادة عدد مستعملي شبكة الأنترنت حيث فاق عددهم 22.71 مليون جزائري سنة 2019 والذي ازداد بنسبة 12% سنة 2020، 13 مليون مشترك في الأنترنت يوميا، 18 مليون حسابCCP، انتشار التجارة الإلكترونية، تفعيل الحكومة الإلكترونية...الخ، وهي أرقام تعكس خطورة هذا الفضاء الذي أصبح كثير النشاط وعرضة لكل أنواع الجرائم.[1]، فقد تنوعت أشكال الجريمة الإلكترونية بالجزائر بين السب والقذف، الإحتيال الإلكتروني الإختراق، السرقة عبر الأنترنت، إعتداء على الأنظمة المعلوماتية والبريد الإلكتروني والمواقع إلكترونية للمؤسسات وغيرها.

وفيما يلي بعض الإحصائيات التي سجلت من طرف الأجهزة الأمنية الجزائرية والتي لا تتعدى بعض التصريحات أو التقارير الصادرة عن الهيئات المخولة بمحاربة هذا النوع من الجرائم، والجدول التالي يبن عدد الجرائم الإلكترونية في الجزائر المسجلة من قبل الأمن الوطني خلال الفترة 2017–2019، حسب أنواعها:

---

[1] Digital 2020 Algeria (January 2020) v01

على الموقع الإلكتروني: /https://www.slideshare.net/DataReportal بتاريخ: 2020/10/05 على ساعة 22:00 .

الجدول رقم 01: الجرائم الإلكترونية في الجزائر في الفترة 2017-2019

السنة / نوع الجريمة	2017	2018	2019
جرائم المساس بالأشخاص عبر الأنترنيت	1511	2410	225
جرائم المساس بأنظمة المعالجة الآلية للمعطيات	28	189	1152
جرائم الإحتيال عبر الأنترنيت	47	149	68
جرائم الإخلال بالنظام العام	/	383	225
جرائم بيع السلع المحضورة على شبكةا لانترنيت	/	203	90
جرائم أخرى	544	188	13
مجموع القضايا المسجلة	2130	3522	1773
مجموع القضايا المعالجة	1570	2677	1402
نسبة القضايا المعالجة	73.71	74.95	79.05

المصدر: زينب نافع، مجيد شعباني: "تحديات الحكومة الإلكترونية في الجزائر، الجريمة الإلكترونية نموذجا". **مجلة العلوم الاقتصادية والتسيير والعلوم التجارية**، العدد 01، المجلد 13، 2020، ص 787.

- من خلال الجدول رقم 01 نلاحظ أن عدد الجرائم الإلكترونية في الجزائر، في تزايد مستمر من سنة لأخرى، فبعدما تم تسجيل 2130 جريمة إلكترونية في سنة 2017، ارتفع عددها في 2018 بـ 1392 جريمة إلكترونية، لتواصل عدد الجرائم المسجلة في الإرتفاع سنة 2018 إلى 3522 جريمة، أما خلال السداسي الأول من 2019 فقد تم تسجيل 1773 جريمة إلكترونية، وهو ليس بالعدد القليل .
- من خلال الجدول السابق نلاحظ أن أنواع الجرائم في الجزائر بالنسبة لسنتي 2017 و2018 تتصدر جرائم المساس بالأشخاص عبر الأنترنت قائمة الجرائم المرتكبة، بنسب تقدر بـ 71%

68%، أما السداسي الأول منسنة 2019، تتصدر جرائم المساس بأنظمة المعالجة الآلية للمعطيات قائمة الجرائم المرتكبة، بنسبة تقدر بحوالي 65% وهذا مقارنة بأنواع الجرائم الأخرى.

وعلى مستوى المصلحة المركزية لمكافحة الإجرام السيبراني للدرك الوطني عالجت المصلحة من بداية سنة 2018 إلى شهر نوفمبر 1140 قضية متعلقة بالجريمة الإلكترونية، منها 136 قضية خاصة بالأطفال[1]، كما سجل مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابع للقيادة العامة للدرك الوطني في سنة 2017 ما يزيد عن 900 قضية جريمة إلكترونية تتعلق أساسا بالقرصنة والإحتيال عبر شبكة الأنترنت[2] منها :

- تعرض موقع قاعدة بيانات وزارة البريد لعملية قرصنة سنة 2016 وتكررت العملية على مستوى إتصالات الجزائر سنة 2017.
- تعرض موقع وكالة الأنباء الجزائرية في الخارج للقرصنة في شهر مارس 2017.[3]

كما كشفت إحدى الدراسات بعنوان بارومتر 2018 حول الأمن السيبراني في المؤسسات الجزائرية عن إحصائيات تكشف التهديدات السيبرانية الموجهة ضد المؤسسات الجزائرية:[4]

– 27 % من المؤسسات التي شملها سبر الآراء تعرضت لاختراق أنظمة معلوماتها خلال 12 شهر بواسطة فيروسات، 15% فقدت بياناتها جراء أخطاء بشرية.

- **دراسة مقارنة حول الجريمة الإلكترونية في الجزائر:**

تعد دراسة موقع comparitech.comسنة 2019 من أهم الدراسات الدولية التي اهتمت بمدى انتشار الجرائم الإلكترونية في العالم، ومن أجل معرفة خطورتها على الجزائر، كان لابد علينا مقارنتها مع

---

[1] الدرك يدعو ضحايا "**الابتزاز الافتراضي**" إلى التبليغ عن المتورطين" 2018/11/27، على الموقع، https://www.tsa-algerie.com، تم الإطلاع على صفحة الويب بتاريخ 2020/10/07 على الساعة 12:00.

[2] وكالة الانباء الجزائرية: "**الجريمة الإلكترونية**". معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني. على الموقع الإلكتروني للوكالة http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018 بتاريخ: 2020/10/11 على الساعة 20:00.

[3] "**الجرائم الإلكترونية تهدد أمن الجزائريين**"، 2018/04/10، على الموقع: https://www.djazairess.com/akhbarelyoum/240271، تم الإطلاع على صفحة الويب بتاريخ 2020/10/13 على الساعة 19:30.

[4] "الأمن السيبراني بالجزائر" **مجلة الجيش**، العدد: 663، الجزائر، أكتوبر 2018، ص44.

بعض دول الأخرى، وقد اعتمدنا هذه الدراسة المقارنة، حول مدى توفر الأمن الإلكتروني في دول العالم، أين شملت 60 دولة من بينها دول عربية وأخرى أجنبية، معتمدة على دراسة سابقة لشركة kaspersky حول نفس الموضوع ،وقد جاءت الدول التي تحصل على أكبر نسبة يكون أمنها الإلكتروني ضعيف وبالتالي هي أكثر عرضة للجرائم الإلكترونية، أما الدول التي تتحصل على أصغر نسبة، يكون أمنها الإلكتروني قوي وبالتالي هي أقل عرضة للجرائم الإلكترونية.[1]

والجدول التالي يوضح بعض الدول التي شملتها الدراسة، والتي من بينها الجزائر.

الجدول رقم 02: معدل انتشار الجرائم الإلكترونية في الجزائر ودول أخرى

المرتبة	البلد	معدل انتشار الجريمة الإلكترونية
1	الجزائر	%55.75
20	مصر	%39.03
23	الإمارات العربية المتحدة	%36.88
25	المغرب	%36.47
27	تونس	%35.57
32	المملكة العربية السعودية	%32.99
60	اليابان	%8.81

المصدر: زينب نافع، مجيد شعباني: "تحديات الحكومة الإلكترونية في الجزائر، الجريمة الإلكترونية نموذجا". **مجلة العلوم الاقتصادية والتسيير والعلوم التجارية**، العدد 01، المجلد 13، 2020، ص 789.

من خلال دراسة النتائج يلاحظ مايلي:

- احتلال الجزائر المركز الأول في معدل انعدام الأمن الإلكتروني من بين 60 دولة شملتهم الدراسة، بمعدل يقدر ب 55.75 %، وهذا يدل على أنها الدولة الأكثر عرضة للجرائم الإلكترونية.

[1] زينب نافع، مجيد شعباني: "تحديات الحكومة الإلكترونية في الجزائر، الجريمة الإلكترونية نموذجا". **مجلة العلوم الاقتصادية والتسيير والعلوم التجارية**، المجلد 13، العدد01، 2020، ص 789.

- بالنسبة للدول العربية الأخرى، تنخفض معدلات انتشار الجرائم الإلكترونية مقارنة بالجزائر، فنجده في تونس 35.57 % في المغرب 36.47% في المملكة العربية السعودية32.99%.
- تتذيل اليابان جميع الدول 59 الأخرى التي شملتهم الدراسة بمعدل 8.81% وتكون بذلك الأكثر أمنا إلكترونيا والأقل عرضة للجرائم الإلكترونية.[1]

المطلب الثاني: الإرهاب الإلكتروني في الجزائر.

يعتبر الإرهاب الإلكتروني من أخطر الجرائم التي يمكن أن يتعرض لها أي بلد في العالم وهذا ما يجعل الجزائر ليست خارج دائرة الخطر، نظرا لإعتماد الجماعات الإرهابية على أحدث الوسائل التكنولوجية في أعمالها التخريبية، كوسائل التواصل الإجتماعي والمنتديات وغيرها، حيث تستخدمها من أجل نشر الافكار الهدامة والتخريبية، كما تقوم بنشر كل أشكال انواع العنف والتطرف في المجتمع.[2]

حيث أن الجماعات الإرهابية تعمل بصورة دائمة ومستمرة على استهداف أمن الجزائر، وهذا ما صرحت به بعض الأجهزة الأمنية وفقا لما أفاد به مصدر أمني مأذون لـ جريدة " **البلاد** " بما يلي:[3]

- ✓ سجلت الأجهزة الأمنية خلال الثلاثي الأول من سنة 2017 أزيد من 2000 تبليغ عن أنشطة متصلة بالإرهاب عبر المواقع الإلكترونية وأغلب هذه التبليغات تتعلق بمحاولات اختراق حسابات مواقع التواصل الإجتماعي أو دعوات للتجنيد في صفوف تنظيمات مجهولة أو إرهابية أو طوائف دينية.
- ✓ سيطرة تنظيم " داعش " على عدد من المواقع والمنتديات الإلكترونية، التي تحتوي عدد كبير من المشاركين تختص بالإيديولوجيا والخطاب وآليات التجنيد والتمويل والتدريب والتخفي وصنع المتفجرات وكل ما يلزم " الإرهابيين".

---

[1] زينب نافع، مجيد شعباني، المرجع السابق، ص 789.

[2] عنتر بن مرزوق ، محمد الكر :"البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب". **مجلة العلوم الانسانية والإجتماعية** ، العدد 38، 2018، ص 38.

[3] الإرهاب الإلكتروني يهدد الجزائر"، 2017/05/13، تم الإطلاع على صفحة الويب 2018/12/01، على الرابط: https://www.elbilad.net/article/detail?id=70386 تاريخ الزيارة 2020/10/13 على الساعة 23:00.

✓ كشفت ذات المصدر أن تنظيم " داعش " لديه فريق من التقنيين متخصص في عمليات الإختراق للبريد الإلكتروني وهتك أسرار الأشخاص والإطلاع على معلوماتهم والتجسس عليهم ممن أجل استغلال تلك المعطيات في عمليات إرهابية.

ومن هنا يمكننا أن ندرك خطر الإرهاب الإلكتروني الذي يمكن أن تتعرض له المؤسسات الحيوية للبلاد ويكون له بالغ الأثر على أمننا القومي وهو ما أكده رئيس الجمهورية السابق السيد عبد العزيز بوتفليقة قائلا: **"لقد أضحى هذا الفضاء الافتراضي تحديا أمنية لبلداننا العربية، خصوصا و أنه يمثل ملاذا للتنظيمات الإرهابية وكل الشبكات الاجرامية لكونه غير مرئي لا سيما تلك التي تنشط في الاتجار بالبشر والأعضاء البشرية والمهاجرين غير الشرعيين والمتاجرة بالمخدرات والأسلحة والمتفجرات وتزوير الهويات والمستندات، فضلا عن دوره في تجنيد المقاتلين الجدد وربط شبكات المقاتلين بعضهم ببعض وتوفير مصادر تمويل خارج الرقابة المنتهجة في إطار تجفيف منابع تمويلها التقليدية".**[1]

كما أكد اللواء مناد نوبة، القائد العام السابق للدرك الوطني الجزائري في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول الأمن السيبراني، حيث قال: **"إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف بإستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الإجتماعي والمنتديات الإلكترونية"** ولذلك دعا إلى إنشاء خلايا أمنية متخصصة تعمل على مراقبة أنشطة المجرمين وتعقبهم ومحاربة كل أشكال الجرائم المتعلقة بالتجنيد الإلكتروني للإرهاب خاصة الشباب، والجريمة المنظمة العابرة للحدود، مع التسلح بالوسائل التكنولوجية الحديثة، من أجل القضاء على الإيديولوجيات المتطرفة والتي تدعو إلى العنف، ضف إلى ذلك ضرورة إعتماد اليات للتعاون بين جميع الشركاء الفاعلين في هذا المجال.[2]

---

[1] وكالة الأنباء الجزائرية: رسالة الرئيس بوتفليقة بمناسبة انعقاد الدورة ال35 لمجلس وزراء الداخلية العرب 2018/03/07. على موقع الوكالة http://www.aps.dz/ar/algerie/54127-35 ، تاريخ الزيارة 2020/10/13.على الساعة 23:30.

[2] الخليج اونلاين، تخصيص خلايا أمنية لتعقب الإرهاب الإلكتروني في الجزائر، من موقع:alkhaleejonline.net بتاريخ: 2020/10/31 على الساعة 21:15.

ومن أهم هذه المواقع الإلكترونية التي تدعو التجنيد والإنضمام إلى صفوف التنظيمات الإرهابية ما يلي:[1]

- **موقع النداء:** يعتبر الموقع الرسمي لتنظيم القاعدة ظهر بعد أحداث الحادي عشر من سبتمبر عام 2001، يتم من خلاله نشر جميع بياناته.
- **ذروة السنام:** وهي صحيفة إلكترونية تابعة للقسم الإعلامي لتنظيم القاعدة.

أما التنظيم الإرهابي "داعش" فإنه يمتلك أزيد من 50 ألف موقع إلكتروني، 90 ألف صفحة باللغة العربية على موقع التواصل الإجتماعي «فيس بوك»، و40 ألفا بلغات أخرى، وهذا ما ساهم في تجنيده حوالي 3400 شاب شهريا عبر حملاته الإلكترونية وهذا حسب تقرير للخبير الأمني في قضايا الإرهاب الرقمي جيف باردين.[2]

---

[1] إيهاب شوقي، الإرهاب الإلكتروني وجرائمه. من موقع:-http://www.assakina.com/awareness net/rebounds/81251.html بتاريخ: 2020/10/31 على الساعة 21:30 .

[2] محمود خليل، 50 ألف موقع إلكتروني لداعش.. والإرهاب يحاصر الأنترنت. من موقع: http://www.alittihad.ae/details.php?id=64991&y=2015&article=full بتاريخ: 2020/10/31. على الساعة 21:30.

المبحث الثاني: آليات مكافحة الجريمة الإلكترونية في الجزائر.

عرفت الساحة الأمنية الجزائرية الكثير من التهديدات التي أفرزتها الثورة التكنولوجية الحديثة والانفتاح على الفضاء الافتراضي، خاصة عبر وسائل التواصل الإجتماعي، حيث أن الجزائر غير معزولة عن دول العالم، ما جعلها تتأثر بكل ما يحيط بها من أحداث وتحديات، عاكفة في نفس الوقت على إعداد النصوص القانونية والمؤسساتية والانخراط بالعديد من الإتفاقيات لمحاربة هذه الجرائم الإلكترونية.

المطلب الأول: الآليات القانونية والإتفاقيات الدولية لمواجهة الجريمة الإلكترونية.

أولا: التشريع القانوني الجزائري:

هناك محاولات جادة من طرف الجزائر لتطوير المنظومة القانونية وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي، حيث سارع المشرع الجزائري باحتواء هذا التطور وإحاطة الجريمة الإلكترونية بأطر قانونية تحكمها.

- ✓ **القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق لـ 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات.**[1]

لقد قام المشرع الجزائري بعمل قيم وهذا من خلال تعديل قانون العقوبات بإدراج القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بمحتوى المادة 394 مكرر إلى 394 مكرر 7 والذي نص على العقوبات التالية:

- **المادة 394 مكرر 1:** عقوبة الإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

- **المادة 394 مكرر2:** عقوبة كل من يقوم عمدا وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن

---

[1] القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتعلق بقانون العقوبات، المؤرخ في 2004/11/10 الجريدة الرسمية، العدد71، ص08.

ترتكب بها إحدى الجرائم المنصوص عليها في هذا القسم، وحيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.[1]

– **المادة 394 مكرر3:** مضاعفة العقوبات المنصوص عليها في هذا القسم، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

– **المادة 394 مكرر 4:** معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

– **المادة 394 مكرر5:** معاقبة كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدة بفعل أو عدة أفعال مادية، بنفس العقوبات المقررة للجريمة ذاتها.

– **المادة 394 مكرر 6:** مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكبت بعلم مالكها.

– **المادة 394 مكرر7:** عقوبة الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.[2]

- ✓ **القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.**[3]

وما يلاحظ على هذا القانون أن المشرع الجزائري عمل فيه على تكيف مواده مع خصوصية الجرائم الإلكترونية، حيث أدرج به 19 مادة تندرج تحت ستة (06) فصول تضمن فصله الأول أهداف القانون ومفهوم المصطلحات التقنية الواردة فيه كالجرائم المتصلة بتكنولوجيا الإعلام والإتصال، منظومة

---

[1] المرجع السابق، ص 12.

[2] المرجع نفسه، ص 12.

[3] القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 2004/08/05، الجريدة الرسمية، العدد 47، الصادرة بتاريخ: 2019/08/16، ص05.

معلوماتية، معطيات معلوماتية، مقدموا الخدمات، المعطيات المتعلقة بحركة السير، الإتصالات الإلكترونية، والأحكام القانونية المتعلقة بمجال تطبيقه والتي تضمن سرية المرسلات والإتصالات، مع وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية، ليتناول الفصل الثاني المادة 4 منه الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية ، حسب ما نصت عليه المادة 3 من هذا القانون.

وأهم ما جاء في الفصل الخامس من هذا القانون هو اقتراح إنشاء هيئة الوطنية للوقاية من الجرائم المتصل بتكنولوجيا الإعلام والإتصال، تتمثل مهامها في محاربة الجرائم الإلكترونية، مصاحبة الأجهزة المختصة في التحريات التي تجريها بشأن هذه الجرائم، جمع المعلومات وإنجاز الخبرات القضائية وتبادل المعلومات مع نظيراتها خارج الاقليم الوطني.[1]

أما الفصل السادس من هذا القانون فتناول التعاون والمساعدة القضائية الدولية مثل تبادل المعلومات حول المجرمين، المحاكم المختصة في الجرائم الإلكترونية المرتكبة خارج التراب الوطني، خاصة من قبل الأجانب الذين يستهدفون المصالح الوطنية، كما وضع المشرع الجزائري شروط في المادة 18 على طلبات المساعدة القضائية والدولية مثل ان لا تكون تمس بالسيادة الوطنية أو النظام العام ومقيدة بشرط المحافظة على سرية المعلومات المبلغة أو عدم استغلالها في غير موضع الطلب.[2]

ويعتبر **القانون 09/04 والقانون 15/10** أهم قانونين سنتهم الجزائر في مكافحة الجريمة الإلكترونية بصفة عامة.

- ✓ **مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الأول عام 1441 الموافق 20 جانفي 2020 والذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية**[3]

المادة الأولى: يهدف هذا المرسوم إلى وضع منظومة وطنية لأمن الأنظمة المعلوماتية.

المادة 2: المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.

---

[1] القانون رقم 09/04، المرجع نفسه، ص 08.

[2] المرجع نفسه، ص 08.

[3] المرسوم الرئاسي رقم 20-05 مؤرخ في 24 جمادى الأول عام 1441 الموافق 20 جانفي 2020 والذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، العدد 04، 26 جانفي 2020، ص 06.

المادة 3: تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، ما يأتي:

– مجلس وطني لأمن الأنظمة المعلوماتية، يدعي في صلب النص "المجلس"، ويكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها.

– وكالة الأمن الأنظمة المعلوماتية تدعي في صلب النص "الوكالة"، وتكلف بتنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

ولممارسة مهامه يتوفر المجلس، بالإضافة إلى الوكالة، على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال.

كما أن المشرع الجزائري أقر أيضا عدة قوانين في مجال الجرائم الإلكترونية والمتعلقة بمؤسسات الدولة وتمثلت في:

- ✓ **قانون البريد والإتصالات السلكية واللاسلكية:** حيث نصت عدة مواد منه فيما يخص المجال السيبراني؛ المادة 87 على سهولة إجراء التحويلات المالية إلكترونيا، والمادة 02/284 على إستعمال حوالات الدفع العادية والإلكترونية، كما نصت المادة 127 على جزاء كل من يفتح أو يخرب بريد.

- ✓ **قانون التأمينات:** وقد نص هذا القانون على تنظيم الجريمة الإلكترونية من خلال مؤسسات وهيئات الضمان الإجتماعي، وذلك في عدة نصوص تخص البطاقة الإلكترونية.[1]

وهذا ما يدل على المجهودات التي ما فتأت تقوم بها لجزائر مند جانفي 2015 ، من أجل تكيف قوانينها التشريعية والتنظيمية مع هذا النوع من الجرائم، وهو ما يتضح من خلال اصدارها لمجموعة من القوانين الخاصة بالتوقيع الإلكتروني والمصادقة الإلكترونية التي من شأنها تطوير الخدمات المقدمة عبر الأنترنت مثل الادارة الإلكترونية، السجل التجاري الإلكتروني، البنوك الإلكترونية وغيرها فضلا عن سعي

[1] يوسف بوغرارة، "الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني". **مجلة الدراسات الافريقية وحوض النيل**، المركز الديمقراطي العربي، المجلد 01، العدد 03، سبتمبر 2018، ص 110.

الجزائر في تطوير قطاع العدالة عبر إرساء قاعدة قانونية لاستخدام التكنولوجيا الجديدة للإعلام والإتصال.[1]

ثانيا: الإتفاقيات الموقعة من قبل الجزائر:

1- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:

حررت هذه الإتفاقية بمدينة القاهرة بتاريخ2010/12/21 وقعت من طرف ممثلي وزراء الداخلية العرب ووزراء العدل لـ 22 دولة، حيث وقع عليها من الجانب الجزائري كل من وزير الداخلية الجزائري دحو ولد قابلية ووزير العدل الطيب بلعيز، تهدف إلى تعزيز التعاون بين الدول العربية لمحاربة جرائم تقنية المعلومات، والتي تهدد سلامة ومصالح المجتمعات العربية وهذا وفق الانخراط في سياسة جنائية مشتركة، عن طريق التعاون والمساعدة الثنائية للوصول إلى تقنية المعلومات المخزنة. [2]

كما نصت المادة 39 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على مايلي:[3]

- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف عن المعلومات التقنية المخزنة والواقعة ضمن أراضي الدولة الطرف المطلوب منها.
- تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفق للأحكام الواردة في هذه الإتفاقية.
- تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل.

---

[1] إسماعيل جنادي: "الأمن السيبراني التحدي القادم للإتحاد الإفريقي". **مجلة الجيش**، العدد: 663، الجزائر، أكتوبر 2018، ص 45.

[2] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، 2010/12/31، ص 25.

[3] نفسه، ص 22.

2- إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي:

لقد صادقت الجزائر على هذه الإتفاقية التي تم إعتمادها من قبل الإتحاد الإفريقي خلال قمته 23 المنعقدة بمالابو بجمهورية غينيا الاستوائية، نظرا للتهديدات الخطيرة التي أصبحت بلدان افريقيا تتعرض لها ووعي القادة الأفارقة بضرورة وضع وتعديل قوانينها وتشريعاتها الإقليمية في مجال الأمن الإلكتروني، على غرار الإتفاقية الأوروبية لبودبست وأهم ما جاء بها:[1]

القرار بشأن تكنولوجيا الإعلام والإتصال في إفريقيا: التحديات والآفاق المستقبلة للتنمية سنة 2010*، إعلان "أوليفر تامبو"، "بتاريخ 09/11/2009"، "إعلان أبيدجان"*بتاريخ 2012/02/22 وإعلان أديس بابا بتاريخ 2012/06/22.

كما تهدف الإتفاقية إلى التنسيق التشريعي بين الدول الأعضاء في مجال تكنولوجيات الإعلام والإتصال، العمل على وضع قوانين تكفل حماية الحقوق الأساسية وضمان الحريات العامة مثل الخصوصية والبيانات الشخصية، كذلك العمل على محاربة الأفعال التي تمس بهذه الحقوق ومعاقبة مرتكبيها [2]، ويتضمن الفصل الثالث من الإتفاقية وضع التدابير الوطنية القانونية والمؤسساتية الواجب اتخاذها بخصوص الأمن الإلكتروني ومحاربة الجرائم الإلكترونية، إضافة إلى النظام الوطني لتأمين الفضاء الإلكتروني، وهذا من خلال ثقافة تأمين الفضاء الإلكتروني ودور الحكومات والشراكة بين القطاعين العام والخاص، وكذلك التعليم والتدريب في مجال أمن الفضاء الإلكتروني.[3]

---

[1] إسماعيل جنادي، مرجع سابق، ص 45.

* الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الإتحاد الإفريقي المنعقدة في أديس بابا بإثيوبيا من 31 جانفي إلى 2 فيفري 2010.

* أعتمد في مؤتمر الإتحاد الإفريقي الاستثنائي للوزراء المسؤولين عن تكنولوجيا المعلومات والإتصالات المنعقد في جنوب إفريقيا بجوهانسبرغ في 2009/11/05.

[2] إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي ملابو غينيا، 2010/06/07، المادة 8، ص 18.

[3] إتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي ملابو غينيا، 2010/06/07، المادة 8، ص 35.

3- الإتفاقية الجزائرية الفرنسية:

عملت الجزائر على وضع كل التدابير والاجراءات اللازمة، بغية محاربة الجرائم الإلكترونية التي جاءت ضمن الإتفاقية الأورو متوسطية المؤرخة في 2002/04/22 وذلك من خلال التنسيق والتعاون المشترك بين دول الوحدة الأوروبية والحكومة الجزائرية.[1] ومن ضمن هذه الدول فرنسا التي وقعت معها في 2003/10/25 بالجزائر على إتفاق تعاون في مجال الأمن ومكافحة الإجرام المنظم، كما نصت المادة الأولى من الإتفاق على إقامة الطرفان تعاون عملياتي وتقني.

المطلب الثاني: البنية المؤسساتية الجزائرية لمكافحة الجريمة الإلكترونية

أولا: المؤسسات الأمنية:

لمحاربة الجرائم الإلكترونية وحماية الامن الإلكتروني الجزائري، كان لابد من إنشاء العديد من الهياكل التنظيمية والهيئات المتخصصة، من أجل مواكبة التحديات الجديدة التي فرضتها التهديدات الآتية من الفضاء الافتراضي، حيث نجد المؤسسات الامنية بكل أجهزتها (الأمن الوطني، الدرك الوطني، الجيش الوطني الشعبي) تلعب دورا مهما في الإستراتيجية الوطنية للقضاء على هذه الجرائم.

1- على المستوى الداخلي:

أ- الدرك الوطني:

✓ قامت فرق الدرك الوطني بإنشاء هياكل لمكافحة الجرائم الإلكترونية ومن بينها نجد:[2]

❖ **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:**

يتكون من إحدى عشر "11" دائرة متخصصة في عدة مجالات، يتمتع بالخبرة التي تأهله لتقديم المساعدات التقنية وتوفير التدريب والتعليم اللازمين لمنتسبيه، كما يعمل على جمع الأدلة الرقمية

---

[1] مختارية بوزيدي: **"ماهية الجريمة الإلكترونية"**. مداخلة ضمن فعاليات الملتقى الوطني أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر العاصمة، 2019/03/29، ص12.

[2] المرسوم الرئاسي رقم 375/07 المتعلق المتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، المؤرخ في 2014/08/05، الجريدة الرسمية، العدد 77، الصادرة بتاريخ 2007/12/09، ص 5-6.

وتسليمها للعدالة ومساعدة المحققين في التحقيق والتفتيش الإلكتروني وهذا ما تتكفل به حصريا دائرة الإعلام الآلي والإلكتروني، والتي تم دعمها بكل التجهيزات مثل بمحطة ترميم و تصليح الأجهزة والحوامل المعطلة، الشبكات الإعلامية و التجهيزات البيانية، محطة محمولة و ثابتة لإجراء خبرات الإعلام الآلي، كما تحتوي سبع قاعات؛ هي كتب التوجبه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، اقتناء المعطيات، قاعة موزع و قاعات تخزين.[1]

ولإنجاز المهمة المنوط بها تنقسم الدائرة إلى ثلاث مخابر وهي: مخبر الإعلام الآلي، مخبر الفيديو، مخبر الصوت.[2]

❖ **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:**

أنشأ هذا المركز سنة 2008، مقره بالجزائر العاصمة، يعمل على حماية وتأمين منظومة المعلومات المتعلقة بأمن البلاد، كما يوثق كل المعطيات الواردة إليه، ويقوم بإجراء دراسة وتحليل البيانات المتعلقة بالجرائم المعلوماتية المرتكبة، بغية التوصل إلى مرتكبيها، وهو ما يوفر الحماية للأنظمة المعلوماتية للمؤسسات الخاصة والعامة مثل البنوك والشركات...إلخ، من مهامه أيضا التنسيق الأمني مع مختلف الشركاء الأمنين، حيث استطاع هذا المركز سنة 2014 معالجة أزيد من 100 جريمة إلكترونية وسنة 2015 معالجة ما يفوق 500 قضية رقمية، ما يعكس نوعية المورد البشري المنتسب إليه والذي اكتسب الخبرة من خلال مشاركاته في الملتقيات الوطنية و الدولية، و تبادل الخبرات مع الدول الأخرى[3].

حيث يسعى المركز إلى:[4]

- تعميم واستكمال نشر فرق المحققين في الجريمة المعلوماتية وتعميم نظام اليقظة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني.
- تكوين مجموعة مختصة في مهام أمن الأنظمة المعلوماتية وحمايتها.

---

1 يوسف بوغرارة، مرجع سابق، ص 111.

[2] إبتسام بغو: **"إجراءات المتابعة الجزائية في الجريمة المعلوماتية"**. مذكرة تخرج مقدمة لنيل شهادة الماستر في القانون، جامعة العربي بن مهيدي أم البواقي، قسم الحقوق، 2015/2016، ص 23.

[3] يوسف بوغرارة، مرجع سابق، ص 111.

[4] العقيد بن رجم جمال، "حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون"، **مجلة الجيش**، العدد: 599، الجزائر، جوان 2013، ص 14.

- تكوين المكونين في المجال وإعداد برامج المواد المتعلقة بالتكنولوجيا الجديدة ومكافحة الجريمة المعلوماتية على صعيد كافة مستويات التكوين.

- يتولى المركز عبر مكاتبه الثلاث مهام التحقيق في الجريمة السيبرانية وتأمين شبكة الأنترنت والأمن الرقمي.
- وفيما يلي إحصائيات الجرائم المعالجة على مستوى المركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.

الجدول رقم 03: تزايد عدد القضايا التي تمت معالجتها على مستوى المركز بين سنة 2008 الى سنة 2019.

سنة معالجة القضايا	2008	2013	2019
عدد القضايا المعالجة	18	102	1652

المصدر: من إعداد الطالب إعتمادا على مجلة الجيش العدد 685، أوت 2020، ص 22.

نلاحظ من خلال الجدول زيادة في عدد القضايا المعالجة على مستوى المركز من 18 قضية سنة 2008 وهي بداية دخوله حيز الخدمة، مع تسجيل إرتفاع في عدد القضايا المعالجة بـ 102 قضية سنة2013 لتبلغ 1652 قضية سنة 2019.

فالتزايد في عدد القضايا المعالجة على مستوى المركز يعكس التركيبة البشرية المؤهلة التي يكتسبها الجهاز من التكوين المستمر لمؤهلين في مجال متابعة وتقصي الجريمة عبر الأنترنت ومن خلال الملتقيات الوطنية والدولية وتبادل الخبرات مع الدول الأخرى في هذا مجال.[1]

[1] سمير بارة: **"الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر 'الدور والتحديات"**. مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني بين التحديات الإقليمية والالتزامات السيادية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، ط2، 30-2017/01/31، ص 435.

ب- المديرية العامة للأمن الوطني:

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:**

أنشأت هذه المصلحة سنة 2011، حيث كانت في البداية عبارة عن فصيلة تابعة مباشرة للمديرية العامة للأمن الوطني، والتي شكلت اللبنة الأولى لمحاربة الجرائم الإلكترونية، ليتم تحويلها في جانفي 2015بقرارمنالسيد المدير العام السابق للأمن الوطني عبد الغاني الهاملإلى مديرية الشرطة القضائية، وهذا تحت تسمية المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.[1]

كما تعمل المصلحة على معالجة مختلف القضايا المتعلقة بالجرائم الإلكترونية على المستوى الوطني والدولي، وقد كانت أول قضية ذات بعد دولي عالجتها بالتعاون مع مكتب التحقيقات الفيدرالية أف بي أي ، وهذا بعد البلاغ الذي تلقته الجزائربخصوصجريمة قرصنة، تعرضت لها شركة أمريكيةحيث تم توجيه الملف إلى مصالح الشرطة القضائية، وبعد التحقيقات تبين أنها منظمة إجرامية تنشط في مجال الإختراق والقرصنة ولها شريك بالجزائر، كما تم التعرف على مكان المجرم وتحديد هويته و تقديمه للعدالة ، ونفس الحالة بالنسبة لاختراق البنك الكندي.[2]

أما على المستوى المحل يفقد تم معالجة العديدمن القضايا المتعلقة بالجريمة الإلكترونية وهذا ما يوضحه الجدول الآتي:

---

[1] سمير بارة: **"الأمن السيبراني (Cyper Security) في الجزائر السياسات والمؤسسات"**. المجلة الجزائرية للأمن الإنساني، العدد 04، جويلية 2017، ص 272-273.

[2] نورة العقون: **"واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر"**. مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة قاصدي مرباح ورقلة، 2019/2018، ص 62.

الجدول رقم 04: يبين عدد القضايا المعالجة على مستوى المديرية العامة للأمن الوطني

السنة	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2013	91	/
2014	245	/
2015	409	347
2016	1055	/
2017	2130	2101

المصدر: من إعداد الطالب إعتمادا على الموقع: www.radioalgerie.dz

نلاحظ من خلال الجدول وتتبع عدد القضايا المعالجة على المستوى الوطني من قبل المديرية العامة للأمن الوطني منذ سنة 2007 إلى غاية 2017، ارتفاع مستمر في عدد الجرائم الإلكترونية حيث تم معالجة 31 قضية سنة 2007 ليرتفع عددها إلى 2130 قضية معالجة سنة 2017، وما يلاحظ أيضا زيادة عدد المتورطين في هذه الجرائممنذ سنة 2007 بتورط 31 شخص ليرتفع إلى 2101 شخص سنة 2017، وقد تنوعت هذه القضايا على النحو التالي:[1]

- 1511 قضية متعلقة بالمساس بالأشخاص كالسب والقذف والمساس بحرمة الحياة الخاصة في الفضاء الافتراضي وقد تعرضلهذا النوع من الإجرام 2381 ضحية.
- 47 قضية متعلقة بجرائم الابتزاز عن طريق شبكة الأنترنت مثل تقديم عروض عمل وهمية للحصول على المال.
- 49 قضية متعلقة بالإعتداء على القصر والأفعال الغير أخلاقية والمخلة بالحياء.

[1] مجلة الشرطة: **"معالجة 2130 جريمة إلكترونية خلال 2017" على الموقع الإلكتروني:** https://www.radioalgerie.dz/news/ar/article/20180417/139053.html بتاريخ: 2021/06/05 على الساعة 18:45.

- 28 قضية إعتداء على الأنظمة المعلوماتية والبريد إلكتروني للمؤسسات وخواص من خلال محو أو تغيير البيانات.

❖ **المخابر العلمية للشرطة:** يوجد منها مخبر مركزي بالجزائر العاصمة ومخبرين جهويين في كل من قسنطينة ووهران، تحتوي على فروع تقنية تضم خلية الاعلام الالي التي تختص في الجرائم الإلكترونية.

❖ **فرقة مكافحة الجريمة المعلوماتية:** هي فرق متخصصة توجد على مستوى جميع المديريات الولائية للأمن، مهمتها التحقيق في الجرائم الإلكترونية والتنسيق مع مخابر الشرطة العلمية.[1]

والقضايا المعالجة نوعان مباشرة أو عن طريق تعليمات نيابية.

ج- الجيش الوطني الشعبي:

عملت قيادة الجيش الوطني الشعبي على إلاء أهمية بالغة للمخاطر التي تهدد الأمن الإلكتروني للجزائر وذلك باستحداث مصلحة لمكافحة الجرائم السيبرانية وتتمثل في:

❖ **مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:**

قامت قيادة الجيش الوطني الشعبي بوضع استراتيجية دفاع سيبراني تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل وفعال وبهذا أنشأة القيادة بتاريخ 2015/11/06 على مستوى دائرة الإستعمال والتحضير لأركان الجيش الوطني الشعبي "مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة".[2]

✓ **مهمتها:** تكلف المصلحة بالعديد من المهام أهمها:

التخطيط وإدراج ومتابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الهادفة لتحقيق بفاعلية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الإتصال وكذا منظومات الأسلحة للجيش الوطني الشعبي، إحباط كل محاولة للتجسس على أسرار الجزائر.

---

[1] نعيم سعيداني، مرجع سابق، ص 107.

2 محمد بوكبشة: "الأمن والدفاع السيبراني (أولوية قصوى)". **مجلة الجيش**، العدد 651، الجزائر، أكتوبر 2017، ص35.

وتتمحور إستراتيجية الدفاع السيبراني للجيش حول سبع محاور وهي:[1]

1- **جانب وظيفي وتنظيمي:** من أجل تنفذ خطط الدفاع السيبراني المسطرة ضمن إستراتيجية الجيش الوطني الشعبي لابد من وجود هياكل تنظيمية تضطلع كل منها بوظيفة محددة مسبقا لضمان التنسيق والفاعلية في الأداء.

2- **جانب قانوني:** ضرورة تحين القوانين المعمول بها كي تتماشى مع التشريعات الوطنية والدولية الجديدة المتعلق بإستعمال تكنولوجيا الإعلام والإتصال.

3- **جانب تقني:** يتطلب الاستعداد الدائم من خلال التزود بأحدث المعدات والوسائل التقنية التي تستخدم في حماية الفضاء السيبراني وردع المجرمين.

4- **جانب الموارد البشرية:** من أهم عوامل نجاح إستراتيجية الدفاع السيبراني هو المورد البشري المؤهل والذي يتمتع بالكفاءة المهنية العالية في نفس المجال وهذا يتحقق من خلال التكوين المستمر وتبادل الخبرات من أجل إكتساب الخبرة والجاهزية.

5- **جانب الوقاية والتحسيس:** العمل على تحسيس أفراد الجيش الوطني الشعبي والمواطنين على مدى خطورة التهديدات التي يمكن أن يتعرضوا لها، حيث يكون مصدرها تكنولوجيا الإعلام والإتصال، لذلك عكفت قيادة الجيش على تنظيم للمحاضرات والملتقيات والايام الدراسية عبر كل ولايات الوطن.

6- **جانب البحث العلمي والتطوير:** يعتبر البحث العلمي ضرورة ملحة من أجل مواكبة حجم التهديدات القادمة من الفضاء السيبراني، والتي تتطلب التسلح بالوسائل التقنية الحديثة والمتطورة ، من أجل ضمان استقلالية الجيش في صناعة قدراته الذاتية في الدفاع السيبراني.

7- **جانب التعاون:** إن التعاون الأمني والتقني في مجال الدفاع السبيراني بين الجيش الوطني الشعبي وجيوش الدول الشريكة، يساهم في رفع الجاهزية وإكتساب الخبرات والمهارات التقنية الحديثة، خاصة من منهم أكثر خبرة وتطور في هذا المجال، كذلك تنظيم الملتقيات والمحاضرات مع الخبراء والمهتمين في هذا الشأن.

[1] محمد بوكبشة: مرجع سابق، ص ص 35-37.

2- على المستوى الخارجي:

أ- المنظمة الدولية للشرطة الجنائية " الأنتربول ":

تعمل هذه المنظمة على محاربة جميع أشكال الاجرام عبر التنسيق بين شرطة الدول 182 الأعضاء بها في تجميع البيانات والمعلومات المتعلقة بالمجرمين؛ كما تسهل الإجراءات القضائية المتعلقة بإنابات القضائية الدولية ونشر أوامر القبض على المبحوث عنهم دوليا وتسليم المجرمين، خاصة ما تعلق بالجرائم العابرة للحدود مثل الجريمة الإلكترونية، ونظرا للبعد الدولي لهذا النوع من الاجرام أكدت الجزائر عضويتها الفعالة في المنظمة من خلال مجهوداتها الجبارة.[1]

وهذا ما تم تأكيده في الاجتماع الـ 10 لرؤساء المصالح المختصة في مكافحة الجرائم المعلوماتية لدول الشرق الأوسط وشمال إفريقيا، المنعقد يومي 10 و11 ماي 2017 بفرنسا بتعين رئيس المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال للمديرية العامة للأمن الوطني على رأس مجموعة خبراء "الأنتربول"؛ المختصة في مكافحة الجريمة المعلوماتية وهذا اعتراف من الهيئات الدولية للمستوى العالي والاحترافية التي أضحت تتميز بها الشرطة الجزائرية في مختلف المجالات.[2]

ب- منظمة الشرطة الافريقية "الأفريبول":

تعود فكرة إنشاء آلية الإتحاد الافريقي للتعاون الشرطي "أفريبول" لسنة 2013 بمناسبة انعقاد المؤتمر الاقليمي الافريقي الـ 22 للإنتربول المنعقد بوهران – الجزائر في الفترة الممتدة من 10 إلى 12 سبتمبر 2013؛ حيث حضر كل قادة الأجهزة الشرطية الافريقية وعددها الواحد والأربعون بدعوة من الجزائر ممثلة في شخص السيد المدير العام السابق للأمن الوطني، أين عقد المؤتمر الافريقي للمدراء

---

[1] فضيلة عاقلي: "**الجريمة الإلكترونية ومواجهتها من خلال التشريع الجزائري**". مداخلة ضمن فعاليات المؤتمر الدولي الربع عشر الجرائم الإلكترونية، مركز جيل البحث العلمي، لبنان: طرابلس، 24-2017/03/25، ص133.

[2] **مكافحة الجريمة المعلوماتية: تعيين خبير من الشرطة الجزائرية لترأس مجموعة خبراء الأنتربول"**. وكالة الأنباء الجزائرية، 28 أيار 2017، على الموقع: www.aps.dz، تم الإطلاع على الويب بتاريخ: 2020/10/18 على الساعة 14:15.

والمفتشين العامين للشرطة حول الأفريبول أيام 10، 11 و12 فيفري 2014، ومن خلاله تم إعتماد إعلان الجزائر بخصوص إنشاء آلية الإتحاد الإفريقي للتعاون الشرطي.[1]

من جملة الأسباب التي دعت إلى إنشاء هذه الآلية تفشي ظاهرة الجريمة وإنتشارها في العديد من الدول الإفريقية، خاصة الجرائم المتعلقة بتكنولوجيا المعلومات والإتصالات والتحويل الغير شرعي لرؤوس الأموال والاتجار الغير مشروع بالموارد الطبيعية وممارسات التهريب.[2]

ج- المكتب العربي للشرطة الجنائية:

أنشاء مجلس وزراء العرب المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة العربية.[3]

حيث تعد الجزائر عضو بهذا المكتب الذي تعمل من خلاله على تنفيذ ما جاء في الإستراتيجية العربية لمكافحة الجريمة المعلوماتية والمنبثقة عن توصيات مجلس وزراء الداخلية العرب.

ثانيا: الهيئات الرسمية الأخرى:

1- على المستوى الداخلي:

❖ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها:

تم إنشاؤها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، يوجد مقرها

---

[1] أمين ودرار: "**الشرطة الجنائية الإفريقية الأفريبول**". حوليات جامعة الجزائر 1، المجلد 34، العدد 01، 2020، ص 138.

[2] خديجة خالدي، "آلية الإتحاد الافريقي للتعاون الشرطي " أفريبول". **مجلة العلوم الإجتماعية والإنسانية**، العدد 15، ص68، 69.

[3] أمال بوجليدة، "المعاهدات الدولية المتعلقة بالأنترنت: مكافحة الجريمة الإلكترونية". **مجلة الجيش**، العدد: 650، الجزائر، سبتمبر 2017. ص ص 46، 47.

بالجزائر لدى الوزير المكلف بالعدل[1]، حيث صدر المرسوم الرئاسي في العدد 40 من الجريدة الرسمية الصادرة في 2020/07/18 يتضمن إعادة تنظيم هذه الهيئة وجاء في أحكامها العامة أن الهيئة هي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية موضوعة تحت سلطة رئيس الجمهورية وهي تعكف في إطار المهام المنوطة بها على:[2]

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.
- مساعدة السلطات القضائية المختصة ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال لاسيما من خلال جمع المعلومات والتزويد بها من خلال الخبرات القضائية.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

وتزود الهيئة عند القيام بمهامها بقضاة وضباط وأعوان الشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للإستعلام والأمن والدرك الوطني كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن مساعدتهم في أعمالها شرط إلتزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل.[3]

---

[1] المرسوم الرئاسي رقم 15-261 المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المؤرخ في 2015/10/08، **الجريدة الرسمية، العدد 53، 2015/10/08**، ص16.

2 نسيم بوبرطخ: "ملف الأمن السيبراني بكافة أشكاله". **مجلة الجيش**، العدد 685، اوت 2020، ص 29.

[3] المرسوم الرئاسي رقم 15-261، مرجع سابق، ص17.

2- على المستوى الخارجي:

أ- الإتحاد الدولي للإتصالات:

هو مؤسسة متخصصة تابعة لمنظمة الإتحاد الدولي لتكنولوجيا الإعلام والإتصال تم إنشاؤها سنة 1869 يوجد مقرها بجنيف (سويسرا) وهي تضم أكثر من 193 بلد عضو بالإضافة إلى منظمي قطاع تكنولوجيا الإعلام والإتصال ومؤسسات القطاع العمومية والخاصة والهيئات الجامعية والأكاديمية.[1]

حيث يعمل على تقديم المساعدة للدول الأعضاء في مجال تكنولوجيا المعلومات والبنية التحتية للإتصالات، من خلال تعزيز الأمن السيبراني وتقليص الفجوة الرقمية بين الدول وتشجيع دعم الكفاءة العاملة بالمجال وكذا تطوير تشريعات الأمن السيبراني على المستوى الوطني والدولي، إضافة إلى تقديم الإستشارة لأصحاب المصلحة حول وضع استراتيجية عالمية من اجل التعاون والتنسيق الدولي.[2]

نذكر من إسهامات الجزائر في الإتحاد مشاركتها في الدورة 19 لمؤتمر المندوبين المفوضين الذي يتم فيه تحديد مبادئه الأساسية وتقرير دوره المستقبلي، عقدت من 20 أكتوبر إلى 7 نوفمبر 2014، والتي أبدت فيها معارضته المشروعين تعديل اللوائح وقرارات تم إعتمادها من قبل أعضاء الإتحاد يتعلق الأمر بالقرار 174 تحت عنوان: دور الإتحاد الدولي للإتصالات بخصوص مسائل السياسات العمومية الدولية ذات الصلة بأخطار إستعمال تكنولوجيا الإعلام والإتصال لأغراض غير مشروعة، والقرار 130 تحت عنوان تعزيز دور الإتحاد الدولي للإتصالات في إرساء الثقة والأمن في إستعمال تكنولوجيا الإعلام والإتصال.

ناهيك عن إنتخاب الجزائر عن منطقة إفريقيا، وإعادت إنتخابها عضو بمجلس الإتحاد من أجل مساهماتها المفيدة والفعالة لأشغال الإتحاد الذي تم عقده من 12 إلى 22 ماي 2015 والذي حثت فيه

---

[1] "التعاون الدولي"، د.ت، على موقع وزارة البريد والمواصلات السلكية واللاسلكية: www.mpttn.gov.dz، تم الإطلاع على صفحة الويب بتاريخ: 2020/10/18 على الساعة 20:30.

[2] فاتح حارك، زكريا قطوش:"**تأثير الفضاء السيبراني على السياسة الأمنية للدول نموذج (الولايات المتحدة الأمريكية)**". مذكرة مقدمة لنيل شهادة الماستر، جامعة صالح بوبنيدر قسنطينة 3، كلية العلوم السياسية، الجزائر، 2018/2017، ص 47.

المجتمع الدولي على العمل من أجل تفعيل اللائحة 174 التي تم من خلالها تعيين الإتحاد مشرفا على القيام بتنفيذها.[1]

ب- مبادرة 5+5 دفاع:

وقعت الجزائر في اجتماع باريس المنعقد 2004/09/30على الوثيقة التأسيسية للمبادرة(5+5 دفاع)، وهذا من أجل العمل على توفير مناخ من الأمن والإستقرار في منطقة البحر الأبيض المتوسط،إقامة علاقة الثقة والتفاهم المتبادل بين الدول المبادرة والتعاون الأمني المشترك فيما بينها بالمسائل ذات الاهتمام المشترك، بالإضافة إلى الاستجابة بفاعلية للتحديات التي تعرفها المنطقة وتعتبر الجريمة الإلكترونية من بين محالات التعاون ذات الإهتمام والأولوية في المبادرة وهذا ما يتضح من خلال تبادل الخبرات والمعارف والمشاريع المشتركة التي تنظمها المبادرة سنويا.[2]

حيث نظمت الجزائر 22 و23 أفريل 2015 بالنادي الوطني للجيش ملتقى دوليا حول "الجريمة المعلوماتية: شبكات التواصل الإجتماعي والأمن العمومي" وقد حضر هذا الملتقى ممثلون عن الدول العشر الأعضاء في المبادرة لكل من فرنسا وإسبانيا، وإيطاليا، البرتغال، ومالطا عن الصفة الشمالية المتوسط والجزائر وتونس والمغرب وليبيا وموريتانيا عن الضفة الجنوبية للمتوسط، وممثلو وزارة الداخلية والجماعات المحلية والعدل والبريد وتكنولوجيا الإعلام والإتصال.[3]

ج- مبادرة مركز البحوث والدراسات القانونية والقضائية:

شاركت الجزائر بفريق من خبراء القانون في العديد من دورات أشغال المركز وذلك بمناقشة القوانين والإتفاقيات المطروحة لتكيف مع التطورات التكنولوجية المتسارعة ومن بين المشاريع المنجزة" الإتفاقية العربية لضمان أمن وسلامة الفضاء السيبراني" والتي من تضمنت العديد من المحاور من بينها

---

[1] "التعاون الدولي"، الموقع نفسه، تم الإطلاع على صفحة الويب بتاريخ: 2020/10/18 على الساعة 20:30.

[2] إلهام غازي، "التحديات الأمنية في البحر الأبيض المتوسط". **مجلة الجيش**، العدد: 668، الجزائر، مارس 2019، ص 53.

[3] **إختتام الملتقى الدولي حول الجريمة المعلوماتية بالجزائر**، بوابة افريقيا الإخبارية، 2015/04/23، على الموقع: https://www.afrigatenews.net/a/64852 اطلع عليه بتاريخ: 2020/10/22 على الساعة 01:30

ضرورة تبادل المعلومات بين الأجهزة المعنية وتظافر جهود السلطات القضائية لمكافحة الجريمة السيبرانية.[1]

[1] جمال بوازدية: "الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية –التحديات والآفاق–". **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01 ، الجزائر، أفريل 2019، ص 1286.

المبحث الثالث: التحديات والآفاق في مكافحة الجريمة الإلكترونية بالجزائر.

رغم الهياكل التنظيمية والموارد المالية والبشرية التي وضعتها الدولة تحت تصرف المؤسسات الأمنية بهدف محاربة الجرائم الإلكترونية، إلا أن هذه الأخيرة لا تزال تجد صعوبات وعراقيل جمة في الميدان، ما جعل صانع القرار يزداد قناعة أن مستقبل الأمن الإلكتروني في الجزائر معادلة صعبة، إن لم تكن هنالك إستراتجية وطنية فاعلة ينخرط فيها جميع الفاعلين والمهتمين بهذا المجال.

المطلب الأول: صعوبات ومعيقات الأجهزة الأمنية في مكافحة الجريمة الإلكترونية:

تواجه الأجهزة الأمنية الجزائرية العديد من الصعوبات والتحديات، التي تعيقها في التصدي إلى الجرائم الإلكترونية، يمكن أن نذكر أهمها فيما يلي:[1]

– **التطور التكنولوجي في مجال الأنترنت والإتصالات:** وهو ما يفرض على الأجهزة الأمنية الجزائرية المختصة بأن تساير هذا التطور، سواء من حيث إكتساب التكنولوجيا والتقنية أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانياتها المحدودة، ولذلك يتوجب توفير جميع الامكانات المادية، المالية والبشرية اللازمة للتحقيق الأمن السيبراني.

– **زيادة عدد المشتركين في شبكة الأنترنت:** إنّ زيادة عدد مستخدمي الأنترنت في الجزائر والمقدر بحوالي 13مليون مشترك يزيد في إرتفاع الجرائم الإلكترونية وبالتالي زيادة التهديدات وهذا ما يمثل أعباء اضافية للأجهزة الأمنية التي تعمل على البحث والتحري على المجرمين ومراقبتهم بين كل هذا العدد من الأعداد من المشتركين.

– **الإستعمال الواسع لشبكات التواصل الإجتماعي:** حيث وصل عدد مستعمليها في الجزائر إلى أكثر من07 ملايين مستعمل، وهو ما ساهم بشكل كبير في ظهور أنواع مختلفة من الجرائم الإلكترونية، مثل: القذف، التحرش الجنسي، استغلال القصر، وغيرها، وهو ما يستوجب وضع استراتيجيات جد محكمة لضمان الأمن الإلكتروني عند استخدام هذه المواقع.

[1] ادريس عطية: "مكانة الأمن السيبراني في منظومة الامن الوطني الجزائري". **مجلة مصداقية**، د،ر،ع ، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، 2019، ص 115.

– **عمليات التخفي أثناء إستعمال خدمات شبكة الأنترنت (Proxy):** وهي من أكبر الصعوبات التي يوجهها المحققين في الجرائم الإلكترونية، الأمر الذي يتطلب منهم التعاون مع جهات مختلفة، وإستعمال وسائل وعتاد جد متطور حتى يتمكنوامن رصد وتتبع مسارات المجرم داخل الشبكة المعلوماتية.

– **غياب التنسيق بين الدول والحكومات:** إن من أكبر الصعوبات التي يمكن أن توجيهها الأجهزة الأمنية الجزائرية هو عدم وجود تعاون بين الدول التي يمكن أن تكون لها علاقة بالجريمة الإلكترونية سواء مباشرة أو غير مباشرة كأن يكون التحضير للجريمة قد أعد بإقليم دولة ما أو ان المجرم فر إلي تلك الدولة، وهنا يضطر المحققين إلى الإتصال بالجهات القضائية الاجنبية من لأجل تقديم المساعدة ، إلا انها غالبا لا تستجيب للطلبات المقدمة، خاصة ان لم توجد هناك إتفاقيات ثنائية بين الدولتين، كما ان تضارب المصالح بين هذه الحكومات يحد من إمكانية التنسيق وبالتالي القبض على المجرمين.

– **الاختلاف في التكوين بين المصالح الشرطية:** يختلف تكوين أجهزة الشرطة من دولة إلى أخرى وهذا ما يجعل من الصعب معالجة القضايا وتقديم المعلومات وتبادلها بين الدول.[1] كما يوجد تفاوت في الوسائل والإمكانيات المتاحة لهذه المصالح.

– **تنوع واختلاف النظم القانونية والاجراءات بين الدول،** هناك إختلافات بين الدول في القوانين والإجراءات التي تضبط طرق التحري والتحقيق وتعطيها الشرعية القانونية، حيث كثيرا ما يصادف المحققين إجراء مشروع في دولة وغير مشروع في دولة أخرى.[2]

– **انعدام ثقافة التبليغ لدى مستعملي الأنترنت:** إن أي شخص يستعمل الشبكة المعلوماتية هو عرضة لأن يكون ضحية للمجرمين الإلكترونين، إلا أن تكتمه عن ذلك وعدم إبلاغ المصالح الأمنية المختصة يرجع في الأساس إلى الخوف من المجتمع أو العادات والتقاليد، وهو ما يسهل إفلاتهم من العقاب وبالتالي إنتشار أكثر لهذا النوع من الجرائم.[3]

---

[1] محمد الحبيب عباسي: **"الجريمة المنظمة العابرة للحدود".** أطروحة لنيل شهادة دكتورة علوم في القانون العام، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017/2016، ص 437.

[2] حسين الزهراني شيخة: "التعاون الدولي في مواجهة الهجوم السيبراني". **مجلة جامعة الشارقة للعلوم القانونية**، المجلد 17، العدد 01 ، الامارات العربية المتحدة ، جوان2020، ص 766.

[3] زينب نافع ، مجيد شعباني، مرجع سابق، ص 788.

المطلب الثاني: مستقبل الأمن السيبراني في الجزائر:

لقد بات التهديد السيبراني من أهم التحديات الجديدة أمام السياسة الأمنية الجزائرية الجزائرية خاصة في ظل رغبة السلطات العليا للبلاد التحول نحو المجتمع الرقمي والإعتماد على الحكومة الإلكترونية، وهو الأمر الذي يتطلب إدخال تكنولوجيا المعلومات والإتصال على جميع الأعمال الحكومية وهنا جاء إدراك الأجهزة الأمنية لمدى خطورة تداول هذه المعلومات بشبكة الإتصالات على نطاق وطني ودولي، أين وجب عليها تأمينها من جميع الإختراقات التي يمكن أن تتعرض لها.[1]

لذلك إتجهت الجزائر إلى **إنشاء مركز عملياتي للأمن "SOC"** سنة 2020 بالتعاون بين اتصالات الجزائر ووزارة الدفاع الوطني، والذي يعد مكسب هام بالنظر إلى وظيفته الرئيسية والمتمثلة في ضمان الأمن المعلوماتي لمختلف البنى التحتية المؤسساتية، حيث يعمل هذا المركز على ثلاثة جوانب أساسية تتمثل في: الإستجابة والإستباقية وجودة الأمن، إعتمادا على توفره على رؤية شاملة لكافة مكونات أنظمة الإعلام الآلي لإتصالات الجزائر، كما يتكون من عدة خلايا مهمتها الكشف عن الهجمات ونقاط الضعف المحتملة على تطبيقات ومنصات إتصالات الجزائر ومن ثم معالجتها بطريقة آنية وفي الوقت المناسب وهذا يعد مكسبا للمنظومة الأمنية السيبرانية بالجزائر.[2] التي لم تعرف سابقا مثل هكذا مراكز.

كما عززت المنظومة الوطنية **بالمرسوم الرئاسي 20-05** كآلية مستحدثة ترعاها وزارة الدفاع الوطني كونها وزارة سيادية من مهامها قضايا الأمن السيبراني، تشمل مجلس وطني لأمن الأنظمة المعلوماتية، مكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.[3] والذي ينتظر أن يدعم المنظومة الأمنية في مواجهة التهديدات الإلكترونية المستقبلية.

إضافة لهذا فإن الجزائر مضطرة إلى إتباع التوجهات العالمية الجديدة التي تفرض تحقيق خطة التنمية لعام 2030، وأهداف القمة العالمية لمجتمع المعلومات للفترة ما بعد عام 2015 (wsis+10) على غرار باقية الدول العربية، من جملة هذه الالتزامات نجد تنفيذ الخطط العالمية التنموية، ومجابهة

---

[1] إدريس عطية، نفس مرجع سابق، ص 117.

[2] "**إنشاء أول مركز سيبراني في الجزائر خوفا من الهجمات الاليكترونية**"، نشر بتاريخ: 2020/02/11 على الموقع: https://shihabpresse.com/ اطلع عليه بتاريخ: 2020/11/01 على الساعة 22:00.

[3] فتيحة حزام: "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية". **مجلة الحقوق والعلوم الإنسانية**، المجلد 13 العدد 03، أكتوبر 2020، ص 181.

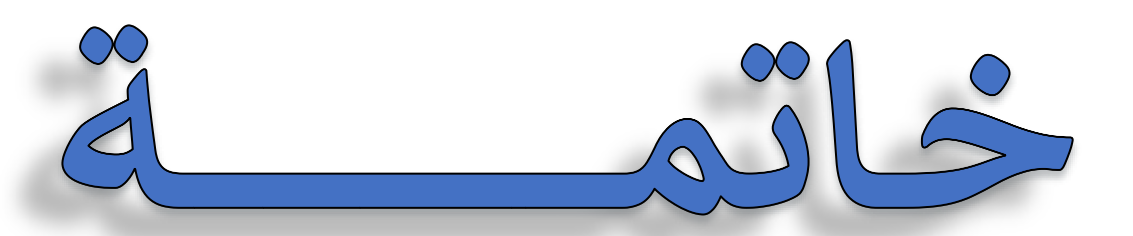
التحديات التي تعيق تنفيذها وذلك من خلال إظهار الالتزام السياسي وتحديث الإستراتجيات خاصة تكنولوجيا المعلومات والإتصالات، بما يتناسب والأهداف التنموية الجديدة ووفقا لأولويات الدول العربية بما فيهم الجزائر.

إذن يجب ألا يقتصر اهتمام الجزائر على الجريمة السيبرانية، بل لابد من إعطاء الأولوية للإرهاب الإلكتروني الدولي والحرب السيبرانية، كون هذا المجال اليوم أصبح ساحة جديد للعمليات السيبرانية، فالقوات المسلحة لا يمكنها العمل دون وجود شبكة اتصالات ومعلومات مؤثرة بها ومرنة لذلك من المهم أن تتمتع الدولة الجزائرية بقدرة على التحكم في هذا الفضاء، حيث يعتبر إطلاق الجزائر أول قمر صناعي للإتصالات بالتعاون مع الصين خطوة مهمة نحو تأمين مؤسساتها وتحقيق الأمن السيبراني.[1]

[1]إدريس عطية، مرجع سابق، ص 117.

خلاصة الفصل الثاني:

إن تزايد عدد مستخدمي الأنترنت بالجزائر و الذي فاق 22.71 مليون جزائري سنة 2019 منهم 13 مليون منخرط في مواقع التواصل الإجتماعي يعكس تزايد التهديدات السيبرانية المتربصة بالبلاد وأمام إرتفاع معدلات الجريمة الإلكترونية بمختلف أشكالها، عملت على محاربتها السلطات العليا على جميع الأصعدة وذلك من خلال إصدار وتحيين القوانين والتشريعات الوطنية التي تتماشى مع القانون الدولي، ومن الناحية الأمنية عملت على إنشاء العديد من الهياكل والفرق الأمنية المتخصصة في الأمن الوطني، الدرك الوطني، والجيش الوطني الشعبي، كما انضمت إلى العديد من المنظمات الإقليمية والدولية ذات الإهتمام المشترك، من أجل توحيد جهودها والإستفادة من تجربة الدول المتطورة في رسم سياسة أمنية وطنية فاعلة وقادرة على تجاوز الكثير من المعيقات التي تقويض دور الأجهزة الأمنية في التصدي لهذه الظاهرة الإجرامية.


خاتمة

لقد إتضح لي من خلال الدراسة التي قمت بها أن نسبة الجريمة الإلكترونية في المجتمع الجزائري إنتشرت بشكل واسع، فلم تعد الحلول والآليات المطروحة من قبل السلطات تستطيع الحد من هذه الظاهرة، خاصة بعد التطور التكنولوجي الهائل الذي تشهده الساحة الدولية، لذلك لابد من تظافر الجهود الوطنية، عبر مختلف الهيئات والمؤسسات الرسمية والغير رسمية، تتقدمها الأجهزة الأمنية التي هي بحاجة إلى البحث عن أساليب وطرق جديدة لمكافحة ومعالجة هذا النوع من الإجرام.

ومن خلال دراستي البحثية توصلت كذلك أنه رغم المجهود الذي تبذله المؤسسات الأمنية (الأمن الوطني، قيادة الدرك، الجيش الوطني الشعبي) في مكافحة الجريمة الإلكترونية، إلا أنها لم تحد من إنتشارها، بل إنها في تزايد مستمر وهذا ما أشرت إليه في دراستي، ونظرا للتطور الحاصل في مجال التكنولوجيا فقد أخذت هذه الظاهرة أشكال وأنواع مختلفة في الفضاء الإلكتروني، كما خلصت إلى أن المصالح الأمنية المتخصصة تعمل على التكيف مع الجريمة الإلكترونية من خلال برامج التحديث والتدريب وإقتناء الأجهزة الحديثة المتطورة، إلا أن هذا لا يكفي إن لم يتم تحديث القوانين والتشريعات التي لا تزال تشوبها عدة ثغرات ونقائص على غرار قانون الإجراءات الجزائية وقانون العقوبات، ضف إلى ذلك عدم وجود أي هيئة مشتركة للأجهزة الأمنية الثلاثة تعمل بالتنسيق ووفق إستراتيجية واحدة ، كما لاحظت أن دور المجتمع المدني والقطاع الخاص مغيب تماما ضمن المنظومة الوطنية المعنية بمحاربة الجريمة الإلكترونية، كما يتضح لنا أن إنخراط الجزائر في الهيئات والمنظمات الدولية يعاني من عراقيل وصعوبات من بينها على سبيل المثال: عدم إلتزام الدول بتطبيق القرارات والتوصيات الصادرة عن هذه المنظمات وتهربها من تسليم بعض المجرمين،وهذا كونها غير ملزمة، ما حال دون وضع إستراتيجية دولية حقيقية وفاعلة في مكافحة الجريمة الإلكترونية .

- **التوصيات والاقتراحات:**

بعد عرض جملة النتائج المتوصل اليها من خلال هذه الدراسة، أمكننا تقديم جملة من التوصيات والاقتراحات التالية:

– وضع إستراتيجية وطنية للوقاية ومحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وضرورة إشراك مراكز البحث العلمي، الإعلام، المجتمع المدني، والقطاع الخاص الى جانب الأجهزة الأمنية المتخصصة.

– تحديث البنية التحتية الوطنية لتقنية المعلومات والإتصالات وحمايتها بأحدث البرامج المتوصل إليها في هذا المجال .

– ضرورة الإستعانة بخبراء في البرامج المعلوماتية والإتصال أثناء القيام بعمليات التحقيق والتقصي في الجرائم الإلكترونية المعقدة والتي تتطلب خبرة علمية عالية.

– ضرورة تكوين وتدريب القضاة ومحققي الأجهزة الأمنية المتخصصة المكلفين بمعالجة قضايا الجرائم المعلوماتية.

– وجوب إنشاء أقسام وغرف خاصة بالمحاكم تختص بمعالجة القضايا الإلكترونية والفصل فيها مع تفعيل التعاون القضائي الدولي.

– الإستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن السيبراني والتعرف على آخر الدراسات التقنية والعلمية للإستفادة منها.

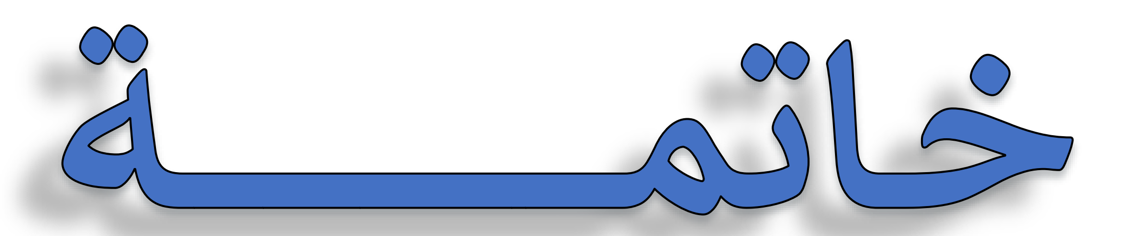
– لابد من خلق آلية تنسيق وتبادل للمعلومات بين مختلف الأجهزة الأمنية من أجل المعالجة السريعة والفعالة للجرائم الإلكترونية التي تمس بالأمن الوطني والدولي.

– تزويد الأجهزة الأمينة المتخصصة بأحدث الوسائل التقنية والبرامج المعلوماتية التي تسهل من عملية التحقيق والتحري حول مرتكبي الجرائم الإلكترونية.

– ضرورة العمل على تحسيس وزرع ثقافة التبليغ لدى مستخدمي الأنترنت من أجل الإخطار الفوري والكشف عن أي أعمال إجرامية يمكن أن يتعرضوا لها أو تمس بالأمن السيبراني للبلاد.

- تعديل قانون الإجراءات الجزائية من خلال إدراج قسم خاص بأعمال البحث والتحقيق في الجرائم الإلكترونية مع تشديد قانون العقوبات في مثل هذه القضايا.

- ضرورة إدراج مادة تربوية في المناهج الدراسية تعنى بتدريس كيفية التعامل الأخلاقي والقانوني والتقني مع تكنولوجيا المعلوماتية.


خاتمة

أولا: المراجع باللغة العربية:

1- الكتب:

1) أحمد خليفة الملط: **"الجرائم المعلوماتية"**. ط2، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
2) اسماعيل قادير،"**ادارة الحروب النفسية في الفضاء الالكتروني**": الاستراتيجية الامريكية الجديدة في الشرق الاوسط، الندوة الدولية: عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، جامعة الجزائر-03-، 2006.
3) أيمن عبد الحفيظ: "**الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية**"، د.ط، دون دار نشر، دون بلد نشر، 2005.
4) جميل عبد الباقي الصغير: "**الجوانب الإجرائية المتعلقة بالأنترنت**".ط2، دار النهضة العربية، الاسكندرية، 2002.
5) جميل عبد الباقي الصغير: "**الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**".ط1، دار النهضة العربية، القاهرة 1998م.
6) حمدون تورية "**الامن السيبراني في البلدان النامية**"، الاتحاد الدولي للاتصالات، 2006.
7) خالد عباد الحلبي: **"إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت"**. ط1، دار الثقافة للنشر والتوزيع، عمان، 2011.
8) ذويب حسين صابر: **"القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع"**. مداخلة بجمعية المكتبات والمعلومات، الرياض 3-2009/11/4.
9) روبرت ماكنمارا، **جوهر الأمن**، ترجمة، يونس شاهين، القاهرة: الهيئة المصرية العامة للنشر، 1971.
10) السيد السليم: **"تطور السياسة الدولية في القرن التاسع عشر والقرن العشرين"**. د.ط، دار الفجر للنشر والتوزيع، القاهرة.
11) طارق إبراهيم الدسوقي عطية: **"الأمن المعلوماتي النظام القانوني للحماية المعلوماتية"**. دار الجامعة الجديدة، الإسكندرية، مصر، 2009.
12) عباس بدارن: **"الحرب الالكترونية، الاشتباك في عالم المعلومات"**. بيروت، مركز دراسات الحكومة الالكترونية، 2010.

13) عبد الحكيم رشيد توبة: "**جرائم تكنولوجيا المعلومات**"، ط1، دار المستقبل، عمان، 2008.

14) عبد الحكيم رشيد توبة: **"جرائم تكنولوجيا المعلومات"**. ط1، دار المستقبل للنشر والتوزيع، الأردن، 2008.

15) عبد الرؤوف مهدي: "**شرح القواعد العامة للإجراءات الجنائية**"، دط، دار النهضة العربية، الإسكندرية، 1996.

16) علاء الدين شحاتة: "**التعاون الدولي لمكافحة الجريمة**"، د.ط، إيتراك للنشر والتوزيع، القاهرة، 2000.

17) محمد أمين أحمد الشوابكة: **"جرائم الحاسوب والإنترنت"**. د.ط، مكتبة دار الثقافة للنشر والتوزيع، عمان، 2004.

18) محمد عبيد الكعبي: **"الجرائم الناشئة عن استخدام الغير المشروع لشكة الإنترنت"**. د.ط، دار النهضة العربية، القاهرة، دون سنة.

19) محمد على العريان: "**الجرائم المعلوماتية**""، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004.

20) محمود أحمد عباينة: "**جرائم الحاسوب وأبعادها الدولية**". دط، دار الثقافة للشر والتوزيع، الأردن، سنة 2005.

21) المعلم بطرس البستاني، محيط المحيط: **قاموس مطول للغة العربية**، مكتبة رياض الفتح: بيروت، سنة 1987.

22) منى الأشقر جبور: **"السيبرانية هاجس العصر"**. المركز العربي للبحوث القانونية والقضائية، بيروت، 2017.

23) منير محمد الجنبيهي وممدوح محمد الجنبيهي: "**جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**"، دط، دار الفكر الجامعي، الإسكندرية، 2004.

24) نائلة عادل محمد فريد قورة: **"جرائم الحاسب الآلي الاقتصادية"**. دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية، 2005.

25) نجيب حسني: "**دروس في القانون الدولي الجنائي**"، القاهرة، د.ط، دار النهضة العربية، 1960.

26) نسرين عبد الحميد نبيه: "**الجريمة المعلوماتية والمجرم المعلوماتي**"، د.ط، منشأة المعارف، الأردن، د.ت.

27) يائير كوهين: **"الفضاء الالكتروني والبعد الخامس للحرب"**. محاضرة في المؤتمر الـ 16 لرابطة الإنترنت الإسرائيلية، مدينة القدس، 2012.

2- المجلات:

28) ادريس عطية: "مكانة الأمن السيبراني في منظومة الامن الوطني الجزائري". **مجلة مصداقية،** د،ر،ع ، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، 2019.

29) إسماعيل جنادي: "الأمن السيبراني التحدي القادم للإتحاد الإفريقي". **مجلة الجيش**، العدد: 663، الجزائر، أكتوبر 2018.

30) اسماعيل زروقة:"الفضاء السيبراني والتحول في مفاهيم القوة والصراع"، **مجلة العلوم القانونية والسياسية**، المجلد10، العدد01، أفريل 2019.

31) إلهام غازي، "التحديات الأمنية في البحر الأبيض المتوسط". **مجلة الجيش**، العدد: 668، الجزائر، مارس 2019.

32) أمال بوجليدة، "المعاهدات الدولية المتعلقة بالانترنت: مكافحة الجريمة الإلكترونية". **مجلة الجيش**، العدد: 650، الجزائر، سبتمبر 2017.

33) الأمن السيبراني بالجزائر" **مجلة الجيش**، العدد: 663، الجزائر، أكتوبر 2018.

34) أمين ودرار: **"الشرطة الجنائية الإفريقية الأفريبول"**. حوليات جامعة الجزائر 1، المجلد 34، العدد 01، 2020.

35) بن عنتر بوزنادة، "تطور مفهوم الأمن في العلاقات الدولية"، **السياسة الدولية**، العدد 160، أفريل 2005.

36) جمال بوازدية: "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات والآفاق–". **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 01 ، الجزائر، أفريل 2019.

37) حسين الزهراني شيخة: "التعاون الدولي في مواجهة الهجوم السيبراني". **مجلة جامعة الشارقة للعلوم القانونية**، المجلد 17، العدد 01 ، الامارات العربية المتحدة ، جوان2020.

38) خديجة خالدي، "آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول". **مجلة العلوم الاجتماعية والإنسانية**، العدد 15.

39) ربيعي حسين: "المجرم المعلوماتي شخصيته وأصنافه". **مجلة العلوم الإنسانية**، العدد 40، جامعة محمد خيضر، بسكرة، جوان2015.

40) زينب نافع ، مجيد شعباني، "تحديات الحكومة الالكترونية في الجزائر، الجريمة الالكترونية نموذجا"، **مجلة العلوم الاقتصادية والتسيير والعلوم التجارية**، المجلد 13، العدد01، 2020.

41) سمير بارة: **"الأمن السيبراني (Cyper Security) في الجزائر السياسات والمؤسسات".** المجلة الجزائرية للأمن الإنساني، العدد 04، جويلية 2017.

a. سـوريــة ديــش: "أنواع الجرائم الإلكترونية وإجراءات مكافحتها". **مجلة العلوم السياسية والقانون**، العدد 01، الجزائر، 2017.

42) عادل عبد الصادق: "الفضاء الالكتروني وتهديدات جديدة للأمن القومي". **مجلة الأهرام لكمبيوتر الانترنت والاتصالات**، مارس 2017.

43) عادل عبد الصادق، "**خطر الحروب السبرانية عبر الفضاء الالكتروني**"، **مجلة الأهرام لكمبيوتر الانترنت والاتصالات**، مارس 2017.

44) عادل عبد الصادق، "القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني". **مجلة السياسة الدولية**، العدد 188، مؤسسة الأهرام، مصر، 2012.

45) عبد الحكيم مولاي إبراهيم: "**الجرائم الالكترونية**"، مجلة الحقوق والعلوم الانسانية، العدد23، جامعة زيان عاشور بالجلفة، الجزائر، سنة 2015.

46) عبد الحميد عائشة وملوك نوال، "الاجرام السيبراني وأثره على تهديد الأمن الثقافي في الجزائر"، **مجلة المفكر للدراسات القانونية والسياسية**: المجلد 3، العدد 3، الجزائر، سبتمبر 2020.

47) عبد العال الديربي ومحمد صادق إسماعيل: **"الجرائم الإلكترونية دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت".** ط1، المركز القومي للإصدارات القانونية، مصر،2012.

48) العقيد بن رجم جمال، "حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون"، **مجلة الجيش**، العدد 599، الجزائر، جوان 2013.

49) عنتر بن مرزوق، محمد الكر: "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الارهاب". **مجلة العلوم الانسانية والاجتماعية**، العدد 38، 2018.

50) فايز بن عبد الله الشهري: "التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة (دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنت)". **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 20، العدد 49، 2005.

51) فتيحة حزام: "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية". **مجلة الحقوق والعلوم الإنسانية**، المجلد13 العدد 03، أكتوبر 2020.

52) محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الالكترونية". **المجلة الأكاديمية للبحث القانوني**، المجلد 14، العدد 02، المملكة العربية السعودية، 2016/11/27.

53) محمد بوكبشة: "الأمن والدفاع السيبراني (أولوية قصوى)". **مجلة الجيش**، العدد 651، الجزائر، أكتوبر 2017.

54) نسيم بوبرطخ: "ملف الأمن السيبراني بكافة أشكاله". **مجلة الجيش**، العدد 685، اوت 2020.

55) نعيمة خطير، "الأمن كمفهوم مطاطي في العلاقات الدولية ...إشكالية التوظيف والتعريف "، **المجلة الجزائرية للأبحاث والدراسات**، المجلد 1، العدد 2، جامعة جيجل، الجزائر، 2018.

56) نورة شلوش، "القرصنة الالكترونية في الفضاء السيبراني- التهديدات المتصاعدة لأمن الدول-"، **مجلة مركز بابل الانسانية**، المجلد 08، العدد02، 2018.

57) يوسف بوغرارة، "الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني". **مجلة الدراسات الافريقية وحوض النيل**، المركز الديمقراطي العربي، المجلد 01، العدد 03، سبتمبر 2018.

3- القوانين والمراسيم التنفيذية:

58) المرسوم الرئاسي رقم 375/07 المتعلق المتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، المؤرخ في 2014/08/05، الجريدة الرسمية، العدد 77، الصادرة بتاريخ 2007/12/09.

59) المرسوم الرئاسي رقم 15-261 المتعلق بتحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 2015/10/08، الجريدة الرسمية، العدد 53، 2015/10/08.

60) القانون رقم 04-15 المعدل والمتمم للأمر 66-156 المتعلق بقانون العقوبات، المؤرخ في 2004/11/10 الجريدة الرسمية، العدد71.

61) المرسوم الرئاسي رقم 20-05 مؤرخ في 24 جمادى الأول عام 1441 الموافق 20 جانفي 2020 والذي يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، العدد 04، 26 جانفي 2020.

62) القانون04.09 المؤرخ في 05 أوت2009، يتضمن " **القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها**" الجريدة الرسمية، العدد47 المؤرخ في 05 أوت 2009.

63) تم وضع ميثاق هذه المنظمة في الفترة ما بين 7-13 جوان 1956 وأعتبر نافذا من 13 جوان 1956.

64) القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المؤرخ في 2004/08/05، الجريدة الرسمية، العدد 47، الصادرة بتاريخ: 2019/08/16.

4- الاتفاقيات:

65) اتفاقية الإتحاد الإفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي ملابو غينيا، 2010/06/07، المادة 8.

66) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، 2010/12/31.

67) اتفاقية حقوق الطفل، النظر في التقارير المقدمة من الدول بموجب الفقرة امن المادة 12 من البروتوكول الاختياري لاتفاقية حقوق الطفل المتعلق ببيع وبغاء الأطفال في المواد الإباحية، لجنة حقوق الطفل، الدورة السابعة والخمسون، 30 ماي 17 جويلية 2011، الأمم المتحدة، رقم:CRC/c/opsc/egy/co/1.

68) اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، رقم (55/63)، الصادرة عن هيئة الأمم المتحدة، الجلسة العامة 81، ديسمبر 2000.

5- المؤتمرات والملتقيات:

69) اجتماع فريق الخبراء المعني بالجريمة السيبرانية، "**مشروع المواضيع المطروحة لنظر في إطار دراسة شاملة بشأن الجريمة السيبرانية وتدابير التصدي لها**". فيينا 17_21 جانفي 2011، رقم UNODC /ccpcj /cg 4/2011/2.

70) جون فرنسوا هنروت: "**أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي**". أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19-20 يونيو 2007.

71) سمير بارة: **"الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر 'الدور والتحديات"**. مداخلة ضمن فعاليات ملتقى سياسة الدفاع الوطني بين التحديات الإقليمية والالتزامات السيادية، كلية الحقوق والعلوم السياسية، جامعة ورقلة، ط2، 30-2017/01/31.

72) عباس أبو شامة عبد المحمود: "**التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية**" الندوة العلمية، الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس أيام 28-30 جوان 1999.

73) فضيلة عاقلي: "**الجريمة الإلكترونية ومواجهتها من خلال التشريع الجزائري**". مداخلة ضمن فعاليات المؤتمر الدولي الربع عشر الجرائم الإلكترونية، مركز جيل البحث العلمي، لبنان: طرابلس، 24-2017/03/25.

74) كريستاس كولمان: "**عن جرائم الانترنيت طبعتها وخصائصها**". الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 يونيو 2007.

75) اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، ورشة عمل حول التشريعات السيبرانية تطبيقها في منطقة الإسكوا، ببيروت 15_16 ديسمبر 2008، المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة، رقم1/ E/ESCWA/ICTD/2009.

76) مختارية بوزيدي: **"ماهية الجريمة الإلكترونية"**. مداخلة ضمن فعاليات الملتقى الوطني أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر العاصمة، 2019/03/29.

77) منى الأشقر جبور:"**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 27-28 أغسطس 2012.

78) مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل 12_19 أفريل 2010، رقم A /conf.213 /9.

79) ندوة التنمية ومجتمع المعلوماتية: **"الجريمة المعلوماتية"**. الجمعية السورية للمعلوماتية، حلب، 2000.

6- الرسائل ومذكرات التخرج:

80) إبتسام بغو: **"إجراءات المتابعة الجزائية في الجريمة المعلوماتية"**. مذكرة تخرج مقدمة لنيل شهادة الماستر في القانون، جامعة العربي بن مهيدي أم البواقي، قسم الحقوق، 2015/2016.

81) أنديرا عراجي: **"القوة في الفضاء السيبراني: فصل عصير من التحدي والاستجابة"**. رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية، جامعة لبنان: كلية الحقوق والعلوم السياسية والإدارية، 2015/ 2016.

82) تركي بن عبد الرحمن المويشر: "**بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليتها**". أطروحة دكتورة الفلسفة الأمنية، جامعة نايف العربية للعلوم الأمنية، الرياض، كلية الدراسات العليا، سنة 2009.

83) رشيدة فاريس، نورة قاوش: **"تأثير مواقع التواصل الاجتماعي في انتشار الجريمة الالكترونية في وسط المراهقين"**. دراسة ميدانية بثانوية كريم بلقاسم بولاية البويرة، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والاتصال تخصص اتصال ومجتمع، جامعة أكلي محند والحاج، كلية العلوم الإنسانية والاجتماعية، قسم العلوم الإنسانية، البويرة، 2018/2017.

84) ريم عميار: " **تأثير الجريمة المعلوماتية على الاقتصاد الوطني**"، مذكرة لنيل شهادة الماستر في الحقوق العام، جامعة العربي بن مهيدي أم البواقي، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2017-2018.

85) العايب أحسن: **" الأمن العربي بين متطلبات الدولة القطرية ومصالح الدول الكبرى 1945-2006"**، أطروحة لنيل درجة الدكتورة في العلوم السياسية، جامعة الجزائر3، كلية العلوم السياسية والاعلام، قسم العلوم السياسية والعلاقات الدولية، سنة 2008.

86) عباسي محمد الحبيب، **"الجريمة المنظمة العابرة للحدود"**. أطروحة مقدمة لنيل شهادة الدكتوراه تخصص القانون العام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، الجزائر، 2017/2016.

87) عبد الرحمن جميل محمود حسين: "**الحماية القانونية لبرامج الحاسب الآلي دراسة مقارنة**". رسالة مقدمة لنيل شهادة الماجستير في القانون الخاص، جامعة النجاح الوطنية، كلية الدراسات العليا سنة 2008.

88) عزيزة رباحي: "**الأسرار المعلوماتية وحمايتها الجزائية**". أطروحة مقدمة لنيل درجة الدكتوراه في القانون، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، سنة 2017-2018.

89) غازي عبد الرحمان هيان الرشيد:"**الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)**". أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.

90) فاتح حارك، زكريا قطوش:"**تأثير الفضاء السيبراني على السياسة الأمنية للدول نموذج (الولايات المتحدة الأمريكية)**". مذكرة مقدمة لنيل شهادة الماستر، جامعة صالح بوبنيدر قسنطينة 3، كلية العلوم السياسية، الجزائر، 2018/2017.

91) فاطمة الزهرة بختي: **"إجراءات التحقيق في الجريمة الالكترونية"**. مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2014/2013.

92) فريال لعقال: **"الجريمة المعلوماتية في ظل التشريع الجزائري"**. مذكرة لنيل شهادة الماستر في القانون العام، جامعة أكلي محند أولحاج البويرة، كلية الحقوق والعلوم السياسية، قسم القانون العام، سنة 2014-2015.

93) محمد الحبيب عباسي: **"الجريمة المنظمة العابرة للحدود".**أطروحة لنيل شهادة دكتورة علوم في القانون العام، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2017/2016.

94) منال مباركي: "**أشكال الجريمة الإلكترونية المرتكبة عبر الفايسبوك**". دراسة ميدانية على عينة من الشباب المستخدمين للموقع في الجزائر، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام والإتصال تخصص اتصال وعلاقات عامة، جامعة العربي بن مهيدي أم البواقي، كلية العلوم الإنسانية والاجتماعية، قسم العلوم الإنسانية، 2017/2016.

95) نايز نبيل عمر: **"الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية دراسة في المحل الإلكتروني المسوغ بالحماية القانونية وبحث المفردات المشمولة بالرعاية وآلية التطبيق في القانون المصري والمقارن".** رسالة مقدمة لنيل شهادة ماجستير في الحقوق، جامعة الإسكندرية، كلية الحقوق، دار الجامعة الجديدة، 2012.

96) نعيم سعيداني: "**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**"، مذكرة مقدمة لنيل شهادةالماجستير في القانون، جامعة الحاج لخضر- باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2013/2012.

97) نورة العقون: **"واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر".** مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، قسم العلوم السياسية، جامعة قاصدي مرباح ورقلة، 2019/2018.

98) يوسف جفال: "**التحقيق في الجريمة الإلكترونية**"، مذكرة لنيل شهادة الماستر في القانون الجنائي، جامعة محمد بوضياف - المسيلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2017/2016.

99) يوسف صغير: "**الجريمة المرتكبة عبر الانترنت**". مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، الجزائر، 2013.

ثانيا: المراجع باللغة الأجنبية:

100) Edward Amoroso, Cyber Security, SiliconPress, 2007.

101) ITU, Cyber security, Geneva: International Telecommunication Union)ITU(,2008

102) MalomAderson policing the world Interpol the politics of international police co-operation clarendon Press .oxford.1989.

103) Mascalacorinne. « Criminalité et contrat électronique » travaux de l'association, CAPITANT. henir journées national .paris 2000.

104) Oxford university press; Oxford word power.(New York :database right oxford university press. 2016.

105) Peter w Singer And Allanfriedam, Cybersecurity And Cyberwar, what Everyone Needls to know, USA:University of oxfordpress, 2014.

106) Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003.

ثالثا: المواقع الالكترونية:

- https://alkhaleejonline.net
- https://political-encyclopedia.org/dictionary.
- https://shihabpresse.com.
- https://www.afrigatenews.net/a/64852
- https://www.alittihad.ae/details.php?id=64991&y=2015&article=full
- https://www.aps.dz.
- https://www.aps.dz/ar/algerie/54127-35.
- https://www.aps.dz/ar/sante-science-technologie/63173-1100-2018.
- https://www.assakina.com/awareness-net/rebounds/81251.html
- https://www.djazairess.com/akhbarelyoum/240271
- https://www.elbilad.net/article/detail?id=70386
- https://www.larousse.fe/dictionnaires/francais/s /s%C3%A9curit%C3%A9/71792
- https://www.mpttn.gov.dz.
- https://www.radioalgerie.dz/news/ar/article/20180417/139053.html
- https://www.slideshare.net/DataReportal.
- https://www.tsa-algerie.com

الملخص:

تعتبر الجريمة الإلكترونية من أحدث وأخطر الجرائم المتواجدة على الساحة الدولية، وذلك لما تشكله من تهديد كبير يمس الأفراد والمؤسسات ويتعداه إلى المساس بأمن الدول وإستقرارها، وهو ما جعل العديد من دول العالم تضع الإستراتيجيات المختلفة للتصدي لهذه الظاهرة والعمل على الحد من مخاطرها، واعتبارها من ضمن أولويات أمنها القومي.

والجزائر على غرار باقي الدول وضعت العديد من الآليات الردعية والعقابية وعزّزتها بهيئات وطنية ومحلية، فالأجهزة الأمنية الجزائرية أنيط لها دور مهم في مكافحة هذه الظاهرة من خلال التحقيق فيها، كشف مرتكبيها، وتسليمهم للعدالة، لذلك وجب على السلطات الجزائرية تدعيم المنظومة الأمنية بالأجهزة التقنية والبرامج المعلوماتية الضرورية للتحقيق أمنها الإلكتروني.

<u>الكلمات المفتاحية</u>: الجريمة الإلكترونية، الأجهزة الأمنية، الفضاء السيبراني، الإستراتيجية الجزائرية، الأمن الإلكتروني.

Summary

Cybercrime or computer-oriented crime is considered as one of the newest and most dangerous crimes in the international arena due to the great threat it poses to both individuals and institutions and it exceeds them even to prejudice the security and constancy of several countries. This is, in fact, what led many countries all over the world to focus on the necessity to confront this phenomenon and work to reduce its risks within the priority of their national security. Among these countries we have Algeria which has developed many deterrent and punitive mechanisms and reinforced them with national and local authorities.

The Algerian security services also play an important role in fighting this phenomenon by investigating it, discovering the perpetrators, and handing them over to justice. Therefore, the Algerian authorities must strengthen the security system using technical equipment and informational programming necessary to reinforce its electronic security system.

<u>Key words</u>: cybercrime, security services, cyberspace, Algerian strategy, cybersecurity.